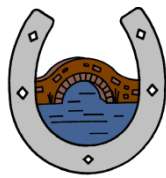


Smithy Bridge Primary School



E-Safety Policy

December 2014

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *Headteacher & Deputy Head teacher*
- *Computing Co-ordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors / Board*

Schedule for Development / Monitoring / Review

This draft e-safety policy is to be approved by the <i>Governing Body / Governors Sub Committee</i> on:	<i>12th February 2015</i>
The implementation of this e-safety policy will be monitored by the:	<i>Senior Leadership Team</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>Governing Body / Governors Sub Committee</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	<i>Annually</i>
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	<i>December 2015</i>
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>LA Safeguarding Officer/MASS/Police</i>

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys / questionnaires of*
 - *pupils*
 - *parents / carers*
 - *staff*

Scope of the Policy

This policy applies to all members of the *Smithy Bridge* community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the *school*.

Governors / Board of Directors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *E-Safety Governor* (Sue Temperley - combined Child Protection / Safeguarding Governor). The role of the *E-Safety Governor / Director* will include:

- *regular meetings with the E-Safety Co-ordinator / Officer*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors*

Headteacher / Principal and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator*.
- **The *Headteacher* and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority HR / other relevant body* disciplinary procedures).
- *The Headteacher & Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher & Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This may involve Rochdale Local Authority if deemed necessary.*
- *The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.*

E-Safety Coordinators / Officers: Mark Brown (Deputy Head & Karen Burman (Computing Leader)

- lead the e-safety committee

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

Smithy Bridge has a managed ICT service provided by an outside contractor, it is the responsibility of the *school* to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the *school* e-safety policy and procedures.

The service provider for Smithy Bridge is EDIT.

Mark Brown & Karen Burman are responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required e-safety technical requirements and any *Local Authority / other relevant body* E-Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person* (see appendix "Technical Security Policy Template" for good practice)

The service provider manages the filtering as per document 'RSN – Internet Filtering' ([see Appendix 1](#))

As per Technical News Updates in Rochdale, EDIT will be changing the way that their filtering works in 2015 – they are moving away from a centralised system to one which is school specific. This will give the school more direct access to filtering and policies in place. This policy will be updated accordingly.

- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

EDIT staff are kept fully up to date on e-safety issues and briefings are regularly delivered. David Brookes from EDIT is currently part of the RMBC LA digital safety group.

- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher or the e-safety officers* for investigation / action / sanction
- *that monitoring software / systems are implemented and updated as agreed in school policies –*

EDIT monitor the use of internet activity as per the document 'RSN – user authentication' ([see Appendix 2](#))

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current *school* e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the *Headteacher or e-safety officers* investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities – Computing policy/e-sense plan & e-sense progression
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Staff receive and sign 'Employee Use of E-Mail, Internet, Personal Mobiles & Rochdale's Intranet' on Induction (see [Appendix 17](#))

Child Protection / Safeguarding Designated Lead

The Designated Safeguarding Lead is Mark Brown and together with Jane George and Karen Burman, he is aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Group

The E-Safety Group Mark Brown, Karen Burman, Trevor Marron (Site Manager) & Sue Temperley (Chair of Governors) provide a consultative group that has wide representation from the *school* community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the *school* this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body*.

Members of the *E-safety Group* will assist with

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

An E-Safety Group Terms of Reference Template can be found in the appendices ([see Appendix 3](#))

Students / pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school

All children from Y2 sign a 'Rules for Responsible Internet Use' ([see Appendix 18](#))

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature*. Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events (please see ICO document 'Data Protection Good Practice Note – taking photographs in school – ([see Appendix 4](#))
- access to parents' sections of the website and on-line pupil records

Parents of children in N-Y1 sign the 'Rules for Responsible Internet Use' ([see Appendix 18](#)) on their child's behalf and all parents sign to give permission for the publication of photographs on the website and in local and national press.

Parents should also refer to the document Smithy Bridge Hints and Tips for Parents ([see Appendix 24](#))

Policy Statements

Education – students / pupils

The Smithy Bridge Computing scheme of work has e-safety at the very core of its content. E-safety is included in every single year group and every topic. Please refer to the 'Smithy Bridge e-sense progression' document ([see Appendix 5](#)) and the 'Smithy Bridge e-sense plan' document ([see Appendix 6](#))

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- *Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

E-safety posters and advice will be shared with the children – (see Appendices 22 & 23)

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / information evenings / sessions
- High profile events eg Safer Internet Day
- Reference to the relevant web sites / publications

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
- *E-Safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide e-safety information for the wider community*
- *Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision*

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A programme of e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process. (see Appendix 7)**
- **All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**
- *The E-Safety Coordinator receives regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and reviews guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

Governors take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

Smithy Bridge has a managed ICT service (EDIT) and it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the *school* E-Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues. – Please refer to RSN ‘Acceptable Use’ policy (see Appendix 8)

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users will be provided with a username and secure password by EDIT who will keep an up to date record of users and their usernames. This will be updated nightly and a copy available to the school at O:\UserAccounts\as pupils.csv and staff.csv. Users are responsible for the security of their username and password but are currently not required to reset their password on a regular basis. Smithy Bridge also has generic logins for pupil access (ks1.smithyb, ks2.smithyb, nursery.smithyb, reception.smithyb, pd.smithyb, vi.smithyb & sen.smithyb) which have a unique password which can only be changed via completion of the online form: <http://snrmbs-rsi/tech/Pages/accountpasswords.aspx>. Please refer to RSN ‘Passwords’ document (see Appendix 9)**
- **The Computing Leader is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations** (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs) Where the school buys into EDIT’s Microsoft Licensing Subscription Services, licensing for Microsoft products is maintained by EDIT on behalf of school. EDIT hold the licences for the school servers and client access licensing regardless of whether the school buys into the subscription service or not.

- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the school / academy will need to decide on the merits of external / internal provision of the filtering service There is a clear process in place to deal with requests for filtering changes. Please see RSN 'Internet Filtering' policy ([see Appendix 1](#))
- *The school has provided enhanced / differentiated user-level filtering* (allowing different filtering levels for staff and pupils)
- *School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.* (schools may wish to add details of the monitoring programmes that are used). Please refer to RSN 'User Authentication' policy ([see Appendix 2](#))
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to EDIT – through logging via Helpdesk on helpdesk@edit.org.uk or calling 01706 927777*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software. Please see RSN 'Security' policy ([Appendix10](#))
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices. (as per RSN 'Acceptable Use' Policy – ([see Appendix 8](#)), RSN 'Security' policy – ([see Appendix 10](#))*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* Please refer to RSN 'Approved Software and Use of Portable Storage Devices' policy ([see Appendix 11](#)) and RSN 'Data Handling Procedures and Guidelines' policy ([see Appendix 12](#))

Bring Your Own Device (BYOD)

Smithy Bridge pupils are not allowed to bring their own devices. Any mobile phones brought by children in Y5/6 (for example, if the child is walking home) must be handed in to the teacher every morning to be locked away until 3.30pm.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images – ([see Appendix 4](#))

- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website*
- *Pupil's work can only be published with the permission of the pupil and parents or carers.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data template is available in the appendices to this document. (Schools / Academies should review and amend this appendix, if they wish to adopt it. Schools / Academies should also ensure that they take account of relevant policies and guidance provided by local authorities or other relevant bodies).

The school ensures that:

- **It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort is made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data is fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". See the Smithy Bridge 'Privacy Notice' ([see Appendix 13](#))**
- **It has a Data Protection Policy –**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- **Risk assessments are carried out as necessary**
- **It has clear and understood arrangements for the security, storage and transfer of personal data**
- **Data subjects have rights of access and there are clear procedures for this to be obtained**
- **There are clear and understood policies and routines for the deletion and disposal of data**
- **There is a policy for reporting, logging, managing and recovering from information risk incidents**
- **There are clear Data Protection clauses in all contracts where personal data may be passed to third parties**
- **There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.**

See RSN 'Data Handling Procedures and Guidelines' ([see Appendix 12](#)), RSN 'Backup' ([see Appendix 14](#)) and RSN 'Backup and Disaster Recovery' ([see Appendix 15](#))

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**

- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

Only Y6 children can bring phones to school but are locked away until 3.30pm

	Staff & other adults			Students / Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school		X						
Use of mobile phones in lessons								
Use of mobile phones in social time	X							
Taking photos on mobile phones / cameras		X						
Use of other mobile devices eg tablets, gaming devices		X						
Use of personal email addresses in school, or on school network	X							
Use of school email for personal emails		X						
Use of messaging apps								
Use of social media								
Use of blogs		X						

- When using communication technologies the school considers the following as good practice:
- **The official email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
 - **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
 - **Any digital communication between staff and pupils or parents / carers (email, etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
 - *From Y3, pupils will be provided with individual school email addresses for educational use.*
 - *Pupils are taught about e-safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
 - *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school / academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Please refer to the Smithy Bridge 'Social Networking' Policy (see Appendix 16)

The *school's / academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions Users shall not visit Internet sites, make, post,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X

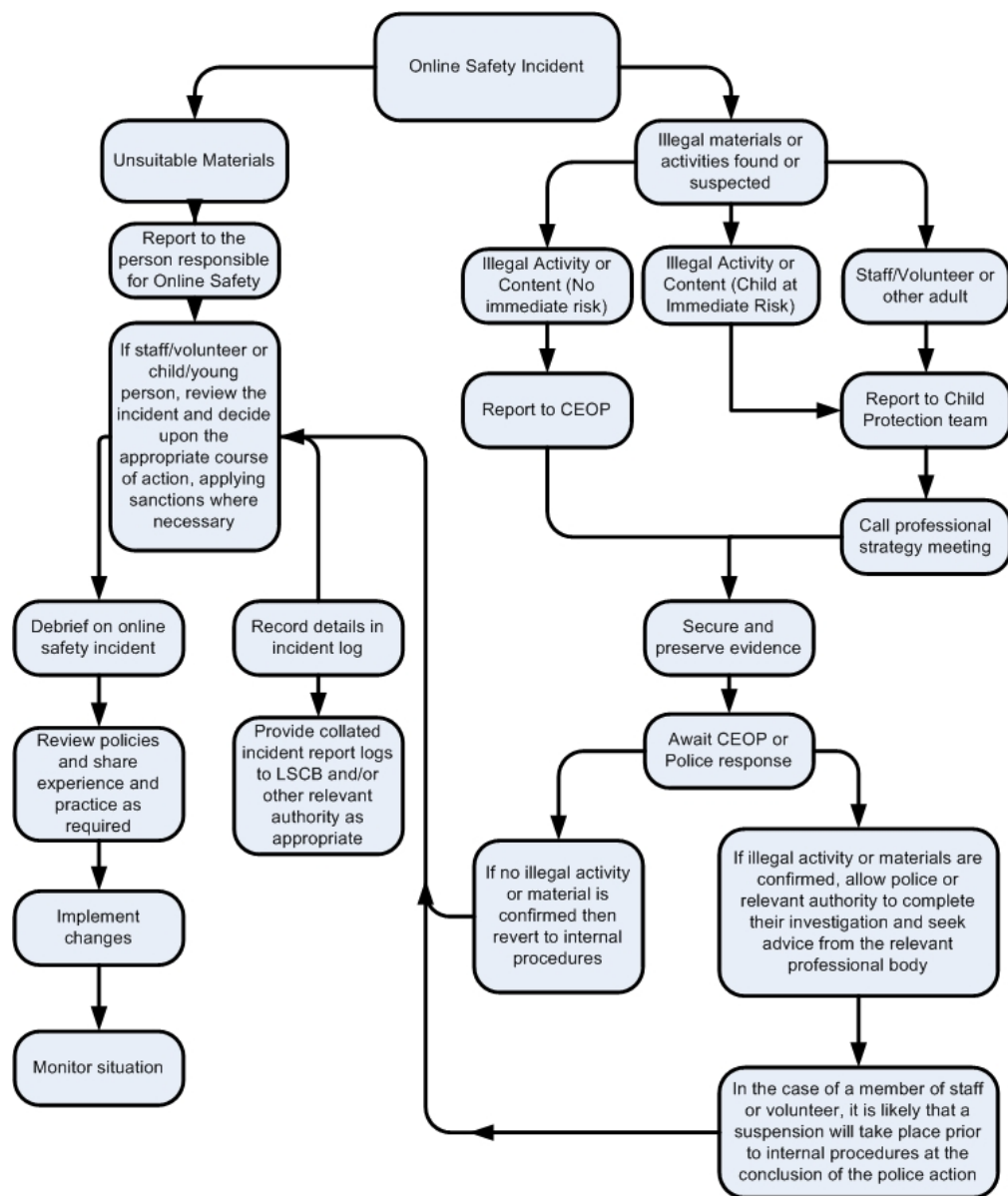
download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing					X	
Use of social media					x	
Use of messaging apps					x	
Use of video broadcasting eg Youtube			x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).

- Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purpose

School Actions & Sanctions –

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Deputy Head & Assistant Head	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X			X			
Unauthorised use of non-educational sites during lessons		X	X			X			
Unauthorised use of mobile phone / digital camera / other mobile device		X	X			X			
Unauthorised use of social media / messaging apps / personal email		X	X			X			

Unauthorised downloading or uploading of files		X	X			X			
Allowing others to access school / academy network by sharing username and passwords		X	X			X			
Attempting to access or accessing the school / academy network, using another student's / pupil's account		X	X			X			
Attempting to access or accessing the school / academy network, using the account of a member of staff		X	X			X			
Corrupting or destroying the data of other users		X	X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X			
Continued infringements of the above, following previous warnings or sanctions		X	X			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X			
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X			X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X			X			

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher/Deputy	Refer to Local Authority (Head's decision)	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X						
Careless use of personal data eg holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security rules		X						

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X						
Actions which could compromise the staff member's professional standing	X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X						
Using proxy sites or other means to subvert the school's / academy's filtering system	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X						
Deliberately accessing or trying to access offensive or pornographic material	X						
Breaching copyright or licensing regulations	X						
Continued infringements of the above, following previous warnings or sanctions	X						

Appendices/Policies

1. RSN 'Internet Filtering'
2. RSN 'User Authentication'
3. E-Safety Group Terms of Reference
4. Data Protection – Good Practice Note on Photographs in School
5. Smithy Bridge E-Sense Progression document
6. Smithy Bridge E-sense Plan
7. E-Safety Training Needs Template
8. RSN 'Acceptable Use'
9. RSN 'Passwords'
10. RSN 'Security'
11. RSN 'Approved Software & Use of Portable Storage Devices'
12. RSN 'Data Handling Procedures & Guidelines'
13. Smithy Bridge 'Privacy Notice 2014-15'
14. RSN 'Backup'
15. RSN 'Backup & Disaster Recovery'
16. Smithy Bridge Social Networking Policy
17. 'Employee Use of E-Mail, Internet, Personal Mobiles & Intranet
18. Smithy Bridge Rules for Responsible Internet Use
19. Record for Reviewing Devices/Internet Sites
20. Template Reporting Log
21. Advice on Safe Search Engines
22. Five SMART Rules for Staying Safe
23. Internet Safety Poster
24. Smithy Bridge Hints & Tips for Parents

Appendix 1 - 'Internet Filtering'



RSN Internet Filtering Policy

1. Introduction

Safety and Security lay at the heart of The Impact Partnership (EDIT) services and the online access that The Impact Partnership (EDIT) delivers across Rochdale Primary, Special and Nursery schools. Filtering is a founding service that is designed to filter out material found to be inappropriate for use in the education environment. Items that infringe filtering policy are blocked and each school adopts a baseline default policy for both staff and students. The Impact Partnership (EDIT) Filtering is powered by BLOXX.

This document summarises methods used to minimise the risks associated with accessing unsuitable and illegal web sites, and our filtering policy designed to help protect against these risks. The document outlines the categories that we filter and provides descriptions of the content deemed inappropriate in each of these categories.

In summary some of the categories included are:

- Adverts
- Alcohol & Tobacco
- Auctions
- Dating
- Drugs
- Gambling
- Gaming
- Hacking
- Hate & Discrimination
- Illegal
- Image Sites
- Offensive & Tasteless
- Peer To Peer
- Pornography & Adult Material
- Proxy Avoidance
- Sex Education
- Software Download
- Spyware
- Streaming Media & Media Downloads
- Violence
- Weapons
- Weblogs & Social Interaction
- Webmail

More information on these categories is provided by this policy document.

Intelligence from industry blacklists are used to build our unique database for education.

2. Use of the Internet in education

93% of Internet users utilise the Internet as a fast and efficient means for gaining information (OxIS, 2007).

It has been proven to “promote effective learning. Students with Internet access have been shown to produce better-researched, more effective and well-presented projects” (Becta, 2007).

Despite the benefits 96% of Internet users believe that there should be restrictions in online content for children (OxIS, 2007).

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound (Becta, 2007).

The key Internet content risks have been categorised by Becta. These categories are outlined in the table below:

Risk	Explanation
Exposure to inappropriate materials	Material that is pornographic, hateful or violent in nature or encourages activities that are dangerous or illegal.
Inappropriate or illegal behaviour	Just as in the real world young people may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. For example online bullying.
Copyright infringement	This could include downloading copyrighted material such as music files, or copying others' homework.
Obsessive use of the Internet and ICT	This could lead to deterioration in the quality of schoolwork or negative impacts upon family relationships.
Physical danger and sexual abuse	This would include paedophiles using Internet chat rooms to target and develop relationships with young people for the sole purpose of sexual activity.
Inappropriate or illegal behaviour by school staff	This could include viewing or circulating inappropriate material.

3. Minimising the risks

By utilising The Impact Partnership (EDIT) Filtering you have already significantly minimised the risks.

In one month at beginning of 2010 we identified and blocked over half-a-million attempts to access web sites that have been classified as unsuitable (06 Jan 2010 to 06 Feb 2010). These web sites would otherwise have been accessed, either inadvertently or by intent if the filtering was not in place.

However, since the content on the web changes so dynamically it is simply not possible for any system based on exclusion to be 100% effective. It is important to understand that filtering is one element in a larger strategy for e-safety and acceptable use.

Becta state that, "Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach. Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, as will their ability for responding to any issues they encounter. Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school and in the home and beyond." (*Safeguarding children online*, Becta, Feb 2009)

Becta highlight this point stating that “no technological solution can be 100 per cent effective in guaranteeing safety when using the internet and related technologies”. Becta advise that that “technology can help to minimise the risks to pupils, particularly when supported by a clear acceptable-use policy and appropriate e-safety education.” This coordinated approach is illustrated below (Figure 1).

The Impact Partnership (EDIT) recommends that the following measures are adopted and used in conjunction with filtering:

- E-safety educational resources and programmes delivered across the whole school community (pupils, staff, governors and parents)
- Appropriate supervision and e-safety education
- Creation and whole-school agreement of clearly defined, agreed and respected e-safety and acceptable usage policy

The combination of these measures provides more complete protection.

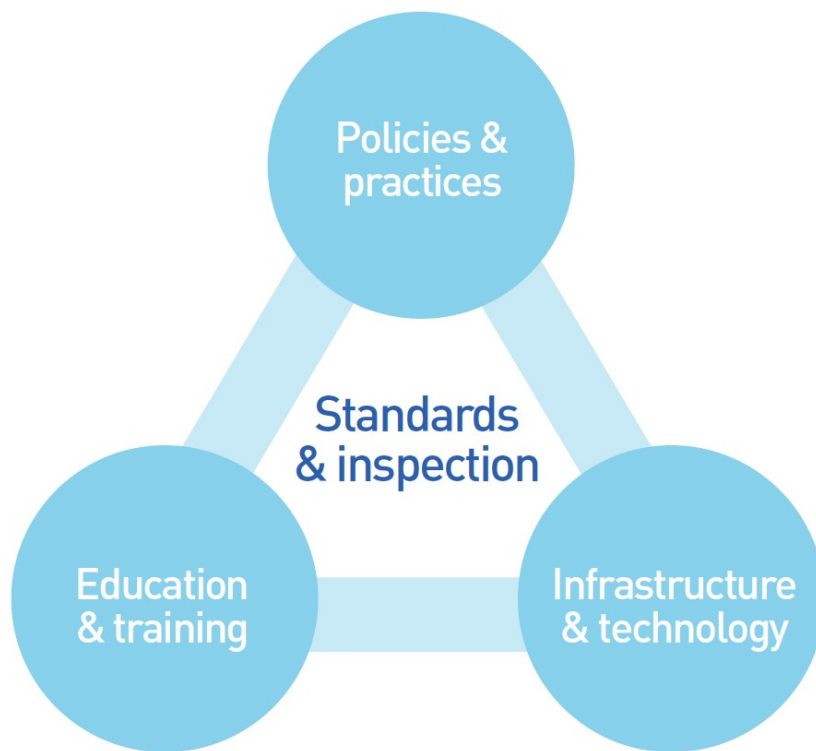


Figure 1: Limiting e-safety risks: Key measures
(from Safeguarding children online, Becta, Feb 2009)

4. Not a 100% Guarantee

Our systems proactively conduct thorough searches in an effort to block user access to any inappropriate material through regular updates from our filtering supplier. However, it is important to understand that we are unable to offer a 100 per cent guarantee in providing an environment that is perceived to be 'safe' by everyone. One reason for this is the constantly changing nature and content of the World Wide Web.

The Impact Partnership (EDIT) block user-access to a large number of unsuitable sites. We do this by the exclusive method, which means that when an inappropriate site is found, The Impact Partnership (EDIT) prevents user access to it. This is in contrast to the inclusive method, which restricts access to all sites, except those identified as appropriate.

Although it is impossible to identify all unsuitable sites, we still believe that the exclusive method is the most suitable Internet filtering policy. Essentially, we believe that the majority of our customers would find the inclusive method too restrictive, as the scope of acceptable sites would be too limiting.

The Impact Partnership (EDIT) Filtering dynamically scans individual web pages for inappropriate content as they are requested using Tru-View technology. This additional protection checks the suitability of pages that have not yet been added to a filter list and categorises them based on the content it finds, providing an additional safety measure which instantly adapts to unsuitable and changing content.

5. Localised Responsibilities

Any activity that could be deemed as 'censorship' has been demonstrated over the years to be a very controversial issue. As the population becomes more risk-aware, we expect over the long term to be using additional mechanisms (e.g. audit logs of use within institutions) in conjunction with varying levels of filtering.

As the Internet is firmly established as a global medium for business, education and entertainment medium, its value is likely to increase perpetually over the years. We suspect the issue of filtering will be with society in general for the foreseeable future, and so we all need to develop our strategies and ideas together.

Use of individualised user credentials to access computerised systems (including the Internet) form part of this strategy so that monitoring and reporting of access issues can be correctly attributed to the activity of

individuals rather than groups. Users of the system therefore need to keep their details secret and ensure they do not leave their workstations 'live' for others to access.

So that establishments can correctly manage their Acceptable Usage Policy, The Impact Partnership (EDIT) provides establishment-based reports on their Internet Filtering activity to named individuals so that local policing and action can be taken if necessary.

Access to local school internet filtering policy is limited to read access only for named individuals. Access to make changes to over-ride the base-default setting to allow or deny access to a website url is granted but for named individuals only with changes only affecting either the staff or the student policy. All usage of the internet filtering administration console is logged and a full audit trail is available to view for system-wide administrators at The Impact Partnership (EDIT). No log file can be deleted or removed without the support and technical assistance of the Internet Filtering Device supplier.

Further information and advice

Becta: <http://schools.becta.org.uk/>









Internet Watch Foundation: <http://www.iwf.org.uk/>

6. Filter Category Definitions and Usage

The Impact Partnership (EDIT) Filtering is designed to filter out material found to be inappropriate for use in the education environment. Items that infringe the filtering policy are blocked by our filtering service.

The Impact Partnership (EDIT) Filtering is customisable offering the ability to tailor your filtering solution in line with your establishment's Acceptable Use Policy. Using this solution it is possible to add to and also to override some of the sites that are filtered. Establishments opting to do this should record these changes in their written policy for all users to acknowledge and understand.

The following is a list of categories that are in place as a base default level for school based filtering.

CATEGORY	STAFF		STUDENT		DESCRIPTION
	WORK	NON-WORK	WORK	NON-WORK	
Adverts					All advertising is placed in this category.
Alcohol & Tobacco					Manufacturers and distributors of alcoholic drinks and tobacco products, as well as websites that promote the use of alcohol or tobacco.

Arts & Entertainment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Music, cinema, theatre, museums, art galleries are all included. Live entertainment venues and comedy clubs. Sites that allow the download of media are explicitly excluded - they are listed under 'Streaming media & media downloads'.
Auctions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Online auction sites, and any site that offers services to aid buying or selling via online auctions - 'auction sniping' etc.
Automotive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Vehicle manufacturers, dealers and servicing are all covered by this category along with road and map sites. Sites that allow traders or the general public to buy or sell vehicles. Clubs for specific manufacturers/models are applicable, as are discussion groups.
Business & Commercial	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Businesses and commercial organisations belong here, as do groups that represent them and any reporting/commentary specifically targeted on this area. Note that IT-related businesses belong to the 'Computers & Internet' category and are not included here.









CATEGORY	STAFF		STUDENT		DESCRIPTION
	WORK	NON-WORK	WORK	NON-WORK	
Computing & Internet	✓	✓	✓	✓	All sites related to computer hardware and software - including sales. News and current trends regarding the computing industry or internet are also applicable. Professional bodies within the IT industry are included. Please note that sites whose main function is to allow users to download software are listed in the 'Software Download' category.
Dating	✗	✗	✗	✗	This category covers matchmaking sites, personal listings, sites that discuss romance and interpersonal relationships - whether partnership is the resultant goal or not. Sites specifically designed for initiating sexual encounters are excluded - these are categorised as 'Pornography & Adult Content'.
Drugs	✗	✗	✗	✗	Sites that sell illegal/controlled substances, promote substance abuse, or sell related paraphernalia.
Education	✓	✓	✓	✓	Colleges, universities, primary and secondary schools are all listed here. Online educational resources, such as exam syllabuses and example questions, are also included. Support organisations such as admissions bodies and research councils.
Finance & Investment	✓	✓	✓	✓	All aspects of personal and corporate finance are included here. Sites that provide price comparisons between financial products. Sites that report or comment on financial matters.
Food & Drink	✓	✓	✓	✓	All sites relating to restaurants (whether eat-in or takeaway) and pubs/bars. All recipes and cuisine related sites are listed in this category. Farms and other foodstuff manufacturers.
Gambling	✗	✗	✗	✗	All online and offline gambling, and sites that promote gambling skills and practice.
Gaming	✗	✓	✗	✓	All sites relating to video, computer or online games. All sites that support gaming through hosting online services, cheat information, general advice etc.
Government	✓	✓	✓	✓	All central and local government websites are applicable, as are related bodies and agencies. Sites related to defence forces such as armies, navies or air forces are not included here - they are listed in the 'Military' category.
Hacking	✗	✗	✗	✗	Resources for the illegal or questionable use of computer hardware or software are listed here, as are sites that promote destructive or malicious software such as viruses and trojans. Sites that describe how to gain unauthorized access to systems. Sites that distribute copyrighted material that has been 'cracked' to bypass licencing.
Hate & Discrimination	✗	✗	✗	✗	Sites promoting aggressive, degrading, or abusive opinions about any section of the population that could be identified by race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice. Political and social groups that discriminate on the grounds of race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice.
Health	✓	✓	✓	✓	All sites related to personal health, hospitals, clinics, legally-prescribed medication and related services.
Illegal	✗	✗	✗	✗	Sites that contain instructions, recipes, or advice on creating illegal items, such as explosives, or offer them for sale. Sites that give instruction on, advice about or promote of illegal acts.

Image Sites	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sites that provide hosting for images.
-------------	-------------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	--

CATEGORY	STAFF		STUDENT		DESCRIPTION
	WORK	NON-WORK	WORK	NON-WORK	
Instant Messaging	✓	✓	✗	✗	Instant messaging clients and services, and any domains required for their successful operation.
Internet Telephony	✗	✓	✗	✓	All sites that offer internet telephony/VoIP products and services.
Lifestyle & Culture	✓	✓	✓	✓	Sites that deal with life issues such as motherhood and raising children. Life events such as marriage and bereavement. Lifestyle choice sites such as gay/lesbian/bisexual are listed here. Sexual content is explicitly excluded and is listed in 'Pornography & Adult Content'.
Military	✓	✓	✓	✓	Sites belonging to official military organisations or containing information relevant to their activities should be placed in this category. Illegal/paramilitary organisations are excluded and should be placed in the Illegal category.
News	✓	✓	✓	✓	All reporting media such as online news, newspapers and current affairs sites are listed here.
Newsgroups & Forums	✓	✓	✓	✓	Sites offering access to Usenet newsgroups or similar services, or any other discussion forum that doesn't sit well in another category.
Offensive & Tasteless	✗	✗	✗	✗	It's not very easy to define exactly what is offensive or tasteless. Sites included are not pornographic or violent; rather, more oriented towards content unsuitable for school children to view or that an employer would be uncomfortable with their staff accessing. Some examples are: discussion of sexual activity of a non-pornographic but explicit fashion; crude humour; images of the casualties from a car crash; defamatory or insulting comments about people, places, religions or cultures.
Peer To Peer	✗	✗	✗	✗	All sites that facilitate the sharing of files using P2P software are placed in this category. This includes, but is not restricted to, sites that host P2P software and sites that allow users to search for files that can be downloaded using via P2P software.
Pornography & Adult Material	✗	✗	✗	✗	Sites containing sexually explicit content in an image-based or textual form. Any other form of adult/sexually-oriented material is also listed here. For example: Escort agencies and swingers clubs; "
Property & Real Estate	✗	✓	✗	✓	All sites oriented to the selling, letting, and building of private or commercial property should be placed in this category.
Proxy Avoidance	✗	✗	✗	✗	Any site that operates as a web proxy, allows access to software that can bypass web filtering, or offers guidance on how web filtering can be avoided is listed in this category.
Recreation & Hobbies	✓	✓	✓	✓	This category covers all activities or interests, other than sport, that someone might pursue for their own pleasure and not as a main occupation. This is obviously a very broad definition.
Recruitment	✓	✓	✓	✓	All employment agencies, recruitment consultancies and headhunters, contractors, and agencies assisting anyone seeking employment are placed here. All sites that allow job vacancies to be posted, offer career advice, describe how to get through interviews or prepare a CV.
Reference	✓	✓	✓	✓	Online encyclopaedias, dictionaries, thesauruses, atlases and other information resources available for research purposes all belong to this category.

Religion	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All sites that relate to religious belief or scepticism should be placed in this category.
----------	-------------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	--

CATEGORY	STAFF		STUDENT		DESCRIPTION
	WORK	NON-WORK	WORK	NON-WORK	
SMS & Mobile Telephony Services					This category is used for sites that allow the creation or sending of SMS text messages. Sites that sell ringtones, games, videos, or other downloadable content. Please note that mobile telephone retailers are not placed in this category - they are listed in 'Shopping'.
Search Engines					This category contains all search engines, meta-search engines and web directories.
Sex Education					This category exists to allow users to access site that discuss sex and sexuality in an informative and non-voyeuristic way. Topics that fall under this category include: education about human reproduction and contraception, sites that offer advice on preventing infection from sexual diseases such as HIV, and sites that offer advice to the LGB communities on sexual health matters.
Shopping					Any site that meets one of the following criteria is listed here: Offers goods for sale; represents a non-online retailer; provides comparisons between goods; preferential purchase schemes. Please note that exceptions are made in the case of sites covered by the other categories: auctions, cars and spares, sexual goods and materials, computer hardware and software, computer and video games, holidays and travel, financial goods and services, alcohol and tobacco, drugs, prescription medicines and weaponry - these are all be placed in the category best suited to the specific purpose.
Software Download					All sites whose main purpose is to allow users to download software, whether on a free or commercial basis.
Sport					All sport websites - whether official, unofficial, media-related or fan-related - are placed in this category, except for those related to gambling.
Spyware					Websites hosting software that attempts to get hold of personal or secret information without the user's knowledge.
Streaming Media & Media Downloads					Any site whose primary function is to allow users to download media content, whether streamed or not.
Translation					All sites that translate a web page from one language to another, or that transform the text contained within a web page, are listed in this category.
Travel					Sites related to the following topics are listed here: - Travel agents. - Airlines, cruise and ferry lines, rail operators, bus and coach companies. - Hotels and holiday rental accommodation. - Travel advice. - Timetable information. - Car hire.
Violence					Any site that displays or promotes content related to violence against humans or animals is placed in this category, as are sites that advocate any means of harming oneself such as self-mutilation or euthanasia.
Weapons					Any site that sells weapons or ammunition or advocates the use of weapons. Sites of weapons manufacturers.
Webchat					Web-based chatrooms.

CATEGORY	STAFF		STUDENT		DESCRIPTION
	WORK	NON-WORK	WORK	NON-WORK	
Weblogs & Social Interaction					Any site that hosts a weblog or lists of weblogs, or provides social networking services is listed in this category. Social networking sites are defined as those that allow users to generate their own profiles or personal content, view the profiles of others, and create links between profiles in order to indicate friendship or approval.
Webmail					Any site offering web-based email services is placed in this category.

A general benchmark used by The Impact Partnership (EDIT) to determine whether a site or part of a site should be filtered, is whether or not the questionable material is something which the national press may publish. If it is, then it is unlikely that The Impact Partnership (EDIT) would choose to filter it.

The default Non-Working times are allocated as:

	SUN	MON	TUE	WED	THU	FRI	SAT	Between
Evening		✓	✓	✓	✓	✓		18:00 – 23:59
Morning		✓	✓	✓	✓	✓		00:00 – 07:00
Weekend	✓						✓	00:00 – 23:59

Changes to these default times are changing by the school by request only to helpdesk@edit.org.uk.

7. Java Authenticated Websites

Where sites use java to authenticate user account permissions (for access to specific content on the website), site urls need to be added explicitly on a global setting which affects all policies.

Sites specifically added are:

clc2.uniservity.com UniServity Learning Platform

8. Review

This Policy will be reviewed on an annual basis. Next review date February 2011.

Appendix 2 - 'User Authentication'



RSN

User Authentication Policy

When things go wrong it is useful to be able to identify the people involved; both the possible victims and those who may have caused the problem. This is as true on computer networks as anywhere else. The aim should be to have all users of RSN identify themselves whenever they are on the network, but in a few situations the cost or inconvenience of achieving this may be unreasonable.

Why identify users?

The *RSN Security Policy* requires that connected organisations exercise 'responsibility about giving, controlling and accounting for access to RSN'. The Policy does not mandate that everyone accessing the network must log on to it, but leaves each organisation to decide how to control network access responsibly.

Likewise, the law of the land and the expectations of society do not insist that every action be traceable to an individual. There is no legal requirement to identify or record every logon, e-mail, web request or mouse click. However activity on a network can almost always be traced to an organisation that owns an Internet domain or address. Organisations are expected to behave responsibly and will be blamed if they are not seen to do so. For example:

- EDIT, The Impact Partnership may, in extreme cases, suspend or withdraw the right to connect to RSN if an organisation's behaviour represents a serious threat to other users of the network;
- other users may be reluctant to accept communications from an organisation that does not deal promptly and effectively with problems, for example some RSN sites may find themselves on blacklists that prevent them exchanging e-mail with others;
- in a few circumstances, the courts may fine an organisation or imprison its decision-making body if crimes were committed as a result of their negligence, in other words, if they have not taken reasonable care to avoid causing foreseeable harm;
- more often, courts may require organisations to pay damages to individuals or businesses who have

suffered loss or harm because of their negligence;

- society and the press may publicly blame an organisation that fails to meet the standards expected of it.

Organisations should consider the risk of misuse when deciding if any groups of users and systems do not need individual identification. An individual account does take time to set up. If the user only needs it for a few seconds then creating and deleting an account may be an unreasonable overhead. However, the convenience of not setting up and managing individual accounts cannot justify a significantly increased risk of harm to others and the organisation. Therefore where generic accounts have been created for use by groups of individuals, access to key systems and files will always be restricted and limited to as few systems as possible.

Harm can be caused by hacking, malicious messages, downloading illegal material and many other types of activity, the scope for which will normally be less where an individual's access is limited to a few systems, rather than the whole Internet. However, if critical internal systems may be accessed then the potential harm should not be underestimated.

How to identify users

The most common way for individuals to identify themselves is to log on when they sit down at a terminal, however this is not the only option. Some organisations let anyone see a limited set of web pages but require a login to gain access to other sites or services. However they are collected, records linking a user to his or her IP address should be kept long enough for misuse to be reported and investigated.

Username and passwords are used to identify individuals. It is therefore paramount that individuals keep these credentials safe and secure to halt impersonation on the network. Staff and students of the organisation should have their own accounts. Visitors may also have local accounts with limited access to the local workstation only. Visitors from other organisations may be authenticated by their home organisation if both organisations are members of RSN.

Even if individual identities are not checked (by use of generic credentials), access to RSN must still be limited to those who are known to the organisation. Knowingly providing network access to strangers is likely to be a breach of RSN policies and to be considered irresponsible by other users of the network.

Access may be limited by physical barriers, although this does not work for wireless networks, or by providing temporary access codes to guests such as conference delegates. Organisations may wish to arrange their networks so that these visitors do not accidentally obtain access to internal resources controlled or licensed by IP address.

Organisations that provide access to networks, and users who benefit from that access, should regard it as normal to require an individual identity. Systems for establishing electronic identity are becoming easier to use and manage. In a few situations there may be a justification for not checking and recording identity but this should only be done after a rational assessment of the risks and benefits.

Organisations should only request individual user credentials for those who are directly related to the long term day-to-day business of the organisation. This includes:

- Staff employed directly by the organisation;
- Pupils registered directly to the organisation.

This does not include those who should be treated as guests to the network with limited access to resources such as:

- Volunteers working on a short-term temporary basis;
- Parents of pupils registered to the organisation;
- Governors or Trustees of the organisation;
- Visitors to the organisation

Appendix 3 - 'E-Safety Committee Terms of Reference'

School Policy Template - E-Safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The e-safety committee will seek to include representation from all stakeholders.

The composition of the group includes

- SLT members
- Child Protection/Safeguarding Designated Lead
- Teaching staff member
- E-safety coordinator
- Governor
- Site Manager

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held termly for a period of 1 hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Co-ordinator (or other relevant person) with the following

- To keep up to date with new developments in the area of e-safety
- To (at least) annually review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through[add/delete as relevant]:
 - Staff meetings
 - Student / pupil forums (for advice and feedback)
 - Governors meetings
 - Surveys/questionnaires for students / pupils, parents / carers and staff
 - Parents evenings
 - Website/VLE/Newsletters
 - E-safety events
 - Internet Safety Day (annually held on the second Tuesday in February)
 - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for have been agreed

Signed by (SLT):

Date: December 2014

Date for review: December 2015

Appendix 4 - 'Taking Photographs in School'

Data Protection Good Practice Note Taking Photographs in Schools

Aim of this guidance

This Good Practice Guidance is aimed at Local Education Authorities and those working within schools, colleges and universities. It gives advice on taking photographs in educational institutions and whether doing so must comply with the Data Protection Act 1998.

Recommended Good Practice

The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the

provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.

Photos taken purely for personal use are exempt from the Act.

Examples

Personal use:

A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.

Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official school use:

Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.

A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Media use:

A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act

Further Information

If you need any more information about this or any other aspect of data protection, please contact us.



Phone: 0303 123 1113

Website: www.ico.gov.uk


Appendix 5 - 'E-Sense Progression at Smithy Bridge'


Planning for progression in ICT and Computing ensures children understand the concepts involved, have learnt techniques and skills and can apply these, as part of a process, to new learning contexts across the curriculum. This ICT progression enables teachers and children to revisit and build on skills and knowledge in a variety of contexts throughout the primary phase ensuring ICT is an integral tool to support learning across the curriculum. The progression in e-sense supports children to make good choices online and develop essential skills for life. It allows them to become safe and responsible participants in the exciting online world that continues to offer new opportunities for learning and play.

	☺Safety	🤝Collaborating	✅Effectiveness and Evaluation	©Copyright			
	Foundation	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
<div>Children understand concepts</div> <div></div>	<p>☺Children recognise the impact of good choices and consequences of wrong ones. Children recognise who they can ask for help and know when they need help.</p> <p>🤝They recognise they can share their learning with others.</p> <p>✅Children are aware that they can use the Internet to play and learn.</p> <p>©Children know that things they create belong to them and can be shared with others.</p>	<p>☺Children begin to understand what personal information is and who you can share it with. Children begin to recognise the need to know who it is they are sharing their learning with online and recognise the difference between real and imaginary online experiences. Children know who to tell when they see something that makes them uncomfortable. Children understand the need for a balance in how they spend their time.</p> <p>🤝Children begin to recognise different ways to communicate online and understand the importance of always being kind and polite.</p> <p>✅Children recognise the Internet as an exciting place to be and begin to make good choices about age appropriate activities. Children understand there are a variety of sources of information and begin to recognise the differences. Children recognise different types of content on websites (e.g. adverts, links) and know that some things may not be true or safe.</p> <p>©Children know that sometimes pictures and words on the Internet cannot be copied because they belong to someone else.</p>	<p>☺Children understand the need for rules to keep them safe when exchanging ideas online. Children understand that any personal information they put online can be seen and used by others. Children recognise excessive use of computers and other devices and begin to consider the need to protect those devices from viruses.</p> <p>🤝Children know they can use online tools to collaborate and communicate with others and the importance of doing this responsibly, including choosing age appropriate websites.</p> <p>✅Children recognise that information on websites may not be accurate or reliable and may be used for manipulation, persuasion or promote bias.</p> <p>©Children understand the need to identify whether material can be shared before using it in their work.</p>	<p>☺Children understand appropriate and inappropriate use of the Internet including excessive use. They recognise the risks and rewards of using Internet communication tools and understand how to protect themselves. They recognise the importance of protecting devices they use from viruses.</p> <p>🤝Children recognise the appropriate online tools to collaborate and communicate with others, understanding how to protect themselves from cyberbullying or causing hurt to others especially when using social networks.</p> <p>✅Children recognise that websites have an author and an audience and some people may publish content that is not accurate. They understand reasons why people might publish content that is not reliable and know they need to check and critically evaluate information. Children recognise the consequences of using unreliable information.</p> <p>©Children recognise the material on the Internet which belongs to someone else and know what can be downloaded to use in their own work.</p>			

<p>Personal Responsibilities</p> 	<p>©Children know their password belongs to them. Children make sure there is an adult with them when using the Internet.</p> <p>▣Children learn to share equipment and take turns.</p>	<p>©Children keep their passwords private. They only play games appropriate for their age. They make sure an adult knows what they are doing online. They tell a trusted adult when they see something that makes them feel uncomfortable.</p> <p>▣Children learn to respect the work of others which is stored on a shared drive of a network or presented online.</p>	<p>©Children keep personal information and passwords private. They choose a secure password. They choose age appropriate games to play on their devices and know when to limit use. Children know they need to be careful about downloading files and games from the Internet. They make sure an adult knows what they are doing online and they know how to report concerns.</p> <p>▣Children respect the ideas and communications of others in work which is presented in an electronic format. They recognise the effect their writing or images might have on others.</p> <p>©Children ask permission to use content created by others.</p>	<p>©Children use social networking websites appropriately, keeping an adult informed about their online activity. They use secure passwords. They make good choices when they present themselves online. They consider the appropriateness of the games they play and the time they spend on different devices. They recognise potential virus threats. Children recognise their right to be safe and happy, and their responsibility to report concerns.</p> <p>▣Children recognise their own right to be protected from the inappropriate use of technology by others. They understand the responsibility for information that is shared and how it may impact on others. They respect the rights of other users.</p> <p>©Children acknowledge where they use other people's content in their own work.</p>
<p>All these are areas which would be a part of a PSHE programme across the school. There are links to the SEAL materials, in particular the themes Going for Goals / Good to be Me.</p>				
<p>Teachers enable progress</p> 	<p>©Teachers model responsible use of ICT resources. Teachers provide opportunities for children to explore onscreen activities that mimic real life. Teachers provide opportunities for children to talk about the</p>	<p>©Teachers talk about the importance of remembering your password and keeping it private. Teachers talk about what is good to put online and what should be kept private. Teachers model appropriate online behaviour when communicating with others including telling an adult about concerns. Teachers develop children's understanding by providing both real and imaginary online experiences. Teachers model closing pop up windows when exploring online resources. They</p>	<p>©Teachers provide opportunities for discussions about the use of communication tools e.g. forums, instant messaging and e-mail. These include opportunities to discuss when an email message or an attachment should not be opened and how to respond when asked for personal details and how to report concerns. Teachers provide opportunities for children to understand that if they make their personal information available online it may be seen and used by</p>	<p>©Teachers provide opportunities to discuss what the consequences might be of sharing personal details online e.g. in a chat room, and how to respond when asked for those details. They discuss the need for careful consideration before downloading attachments to emails or games and the need for virus protection software. They provide opportunities for children to talk about how they use the Internet, how they present themselves online and how they report concerns.</p>

	<p>differences between real and imaginary experiences.</p> <p>Teachers provide opportunities for children to share learning with their families online.</p> <p>Teachers talk about where they find information.</p> <p>Teachers model acknowledging and appreciating the ideas of others.</p>	<p>explain the risks in clicking on these.</p> <p>Teachers provide opportunities for children to share experiences with other learners and experts.</p> <p>Teachers talk about the difference between sources of information e.g. that a CD-ROM has limited information and that websites may feature advertising or links to other areas of the Internet. Teachers prepare hyperlinks for children to access appropriate websites to find information and activities to support learning in a variety of curriculum contexts. They talk about why these websites are good choices. Teachers model the use of age-appropriate search engines and talk about which links to follow and which to avoid on a website. Teachers provide opportunities for children to demonstrate and discuss how they navigate a web site or a piece of software.</p> <p>Teachers model making choices of images and text to use in the classroom.</p>	<p>others. They model making good choices about images to share online.</p> <p>Teachers provide opportunities for children to exchange and develop ideas with other learners and experts in a range of curriculum contexts.</p> <p>Teachers model the analysis of information found on the Internet e.g. from different sources, and the need to check that the information is relevant and accurate, and think about the consequences of errors or omissions. Teachers provide opportunities for children to use the Internet in appropriate contexts to effectively navigate websites. They talk about how to recognise an appropriate website or game.</p> <p>Teachers model how to recognise whether the content on a website can be used without asking for permission.</p>	<p>Teachers provide opportunities for children to exchange and share ideas with a wider audience; talking about the responsibility each individual has when sharing information. They encourage children to evaluate their use of technology including the use of email, social networking, online gaming, and mobile phones.</p> <p>Teachers set challenges to enable children to identify and evaluate differences in information from a variety of sources, both web based and printed texts. Teachers provide opportunities for children to discuss the key features of web sites including their appropriateness. They set challenges for children to construct 'web pages' to enable them to appreciate that anyone can produce and publish a web site. Teachers expect children to be able to work independently, both alone and in groups, with the Internet.</p> <p>Teachers encourage discussion about copyright and intellectual property.</p>
--	---	---	--	---

<p>Children build skills</p> 	<p>©Children explore with real and pretend technology talking about the difference between real and imaginary experiences. Children are supported to use simple passwords to access learning spaces. Children talk about appropriate behaviour when using ICT equipment.</p> <p>✎Children use ICT equipment to send positive messages to others.</p> <p>✓Children look at an appropriate range of image based information to support their learning.</p> <p>©Children choose to share things they've made.</p>	<p>©Children minimise a screen and tell an adult if they encounter a problem on a website. Children use a secure password independently. They talk about the choices they make about the games and activities they play online and with different devices.</p> <p>✎The class add ideas to an online forum and begin to collaborate on simple tasks with their peers.</p> <p>✓Children explore screen-based activities and make choices. They use navigation skills to access different sections of a program and explore sign-posted age appropriate websites using forward and back arrows. They know how to return to the home page when exploring away from a teacher directed site. Children begin to make good choices of useful hyperlinks to other information avoiding links such as advertising. They learn how to undertake simple searches of electronic books using key words and begin to use an age appropriate search engine.</p> <p>©Children create their own images, take photos or choose from a bank of images selected by their teacher.</p>	<p>©Children describe some of the risks and rewards of the Internet. Children know how to behave in order to protect themselves including thinking about the appropriateness of different online experiences and the amount of time they spend on computers or other devices. They begin to consider potential virus threats when downloading files. Children identify what is real and what is imaginary online. They create a secure password and keep it private. They tell an adult if they see content that makes them uncomfortable or they make contact with people they don't know. They choose appropriate images and details to share online.</p> <p>✎Children use online tools such as forums to exchange information and collaborate with others within and beyond their school. They record and share information electronically.</p> <p>✓Children use age appropriate search engines to research and gather different forms of information (text, images, sound and video). Children critically evaluate web sites and describe the possible impact of published content on an audience e.g. the use of advertising and how sites might be designed to persuade and influence.</p> <p>©Children check websites to see whether images, text, video and sound can be copied to use in their work.</p>	<p>©Children use the Internet in ways which minimize risks and discuss the consequences of trusting information and people on the Internet. They make choices about the use of appropriate websites and recognise the need to have virus protection software. They select and use secure passwords. They consider the right to be safe and describe effective ways to report concerns.</p> <p>✎Children select an appropriate tool to collaborate and communicate safely with others within and beyond their school. They begin to evaluate the effectiveness of the tool to support their learning. They consider the impact of information they share with others.</p> <p>✓Children refine searches to obtain appropriate information to support their learning. Children evaluate information from a range of sources, considering its plausibility and developing strategies to make judgements on the sources being used.</p> <p>©Children re-structure and re-present materials in ways which are new and 'unique'; acknowledging the source of copied images, text, sound and video.</p>
<p>Typically</p>	<p>Educational online tools such as Virtual Learning Environments (VLEs)/learning platforms, blogs and discussion boards Somerset e-safety learning resources on www.somersetelim.org</p>			

<p>using</p>	<p>London Grid for Learning esafety Education resources page http://www.lgfl.net/esafety/Pages/education.aspx Safe, digitalMe website http://www.safesocialnetworking.org/getstarted/</p> <p>CEOP Thinkuknow resources: based on Hector's World resources www.thinkuknow.co.uk/5_7/ Hector's World: Australian e-safety activity site http://www.cybersmart.gov.au/Young%20Kids/Hectors%20World.aspx Netsmartz american e-safety resources http://www.netsmartzkids.org Kidsmart: Adventures of Smartie the Penguin http://kidsmart.org.uk/teachers/ks1 Kidsmart: Digiduck's Big Decision http://www.kidsmart.org.uk/teachers/ks1/digiduck.aspx</p> <p><i>Spoof Website for evaluation</i> The Tomato Spider http://webfronter.com/rbkc/tomatospider/</p> <p>CEOP Thinkuknow resources: www.thinkuknow.co.uk/8_10/ Childnet, KnowITall Captain Kara, Winston and the Smart Crew http://www.childnet-int.org/kia/primary/smartadventure CBBC Safesurfing Guide: www.bbc.co.uk/cbbc/help/safesurfing/index.shtml CyberQuoll: http://www.cybersmart.gov.au/cyberquoll/html/menu.html Netsmartz american e-safety resources http://www.netsmartzkids.org Safesurfing with Doug: Disney-based activities for safety issues www.disney.co.uk/DisneyOnline/Safesurfing <i>Spoof Websites for evaluation</i> Dog Island Free Forever: www.thedogisland.com Tree Octopus: http://zapatopi.net/treeoctopus.html</p> <p>CEOP Thinkuknow resources: www.thinkuknow.co.uk/8_10/ Gridclub Cybercafe: http://www.gridclub.com/freearea/tasters/cybercafe/base.htm Learning and Teaching Scotland http://www.ltscotland.org.uk/informationliteracy/9to11/index.asp</p> <p><i>Spoof Websites for evaluation</i> Victorian Robots: www.bigredhair.com/robots/index.html Google Technology: www.google.com/technology/pigeonrank.html All about Explorers http://www.allaboutexplorers.com Petrol Direct http://petroldirect.com</p>
<p>Curriculum contexts</p> 	<p>Curriculum contexts are found in all activities where staff or pupils are using ICT. Children need to see e-sense modelled whenever the Internet is used. See the other ICT Progressions for curriculum contents.</p> <p>Safe sites for children to use for searching the Internet: http://www.bbc.co.uk/cbbc/find http://www.kidsclick.org http://www.askforkids.com http://www.searchbox.co.uk/kids http://kids.yahoo.com http://primaryschoolict.com http://www.swiggle.org.uk</p>

Appendix 6 - 'Smithy Bridge Primary School e-sense/e-safety plan

- Ensure every member of staff has received e-Safety training to be able to recognise and make use of opportunities to raise or reinforce e-Sense messages.
- Ensure every member of staff has read and understood the e-Safety policy.
- Consider effective partnership strategies for inclusion of parents and carers in developing e-Sense for all learners.
- Register and evaluate overall e-Safety with www.360safe.org.uk or other surveys

Activity	Term 1	Term 2	Term 3	Assessment, achievement and evaluation
Assembly	Cyberbullying ☑ I am kind and responsible	Personal safety 😊 I am safe	Excessive/obsessive use 😊 I am safe	Assessment Self, peer and teacher assessments are on-going. Achievements Awards are made to children to recognise responsible behaviour. Evaluation Surveys of parents and carers, children and teachers are used to inform the planning for development of e-Sense. http://bit.ly/esafetysurveys
Whole class lesson (other half of term to assembly)	Reinforce internet rules based on personal responsibilities.	Focus on keeping personal details private, consideration of who you are talking to online and making sure a trusted adult knows what you are doing online.	Consider age appropriate and healthy use of technology (age indicators for games, time spent and sites used.)	
Cross curriculum	<ul style="list-style-type: none">Effectiveness, evaluation and copyright are part of research and presentation tasks across the curriculum.☑ I think carefully: Effectiveness & Evaluation (Reliability, Validity and Bias)© It's not mine: Copyright e-Safety and appropriate communication is talked about as part of all school activities. 😊 I am safe: Safety (Security, Safe Behaviours, Obsessive Use of ICT) ☑ I am kind and responsible: Collaborating (Safe Behaviours, Bullying, Digital Footprint)			
Theme weeks	Anti-bullying week includes cyberbullying messages.	Safer Internet Day is part of a week's focus on the use of the Internet, different devices and technologies.	Health week includes considerations of time spent on the computer and recognition of appropriate websites.	
Partnership with Parents and carers	Pupil/parent AUP and photo permissions for all parents are signed. Leaflet sent home, copies of class agreed Internet rules sent home.	Children create leaflet/poster to take home for parents and carers.	A parent and carers assembly is led by children.	Information available on school website: e-Safety news items included in newsletters.
	An e-Safety meeting for parents and carers maybe planned if it is deemed necessary			

Appendix 7 - 'E-Safety Training Needs Audit'

Training Needs Audit Log Group Date									
Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date			

Appendix 8 - RSN 'Acceptable Use'



RSN Acceptable Use Policy

Background and Definitions

1. **"RSN"** is the name given both to the Rochdale Schools Network – a wide area network to support the requirements of Rochdale Primary, Special and Nursery Schools who buy into an annual service delivered by the Impact Partnership (Rochdale Borough) Ltd. through the EDIT Team.
2. RSN is maintained primarily to support education and communication technologies within Rochdale Primary, Special and Nursery maintained schools. It is not a public network. The *RSN Acceptable Use Policy* does not determine the eligibility of any particular organisation to have a connection to and use RSN. This eligibility is determined by the annual buy back subscription. The RSN Acceptable Use Policy merely defines acceptable and unacceptable use of RSN by those who have been provided with a connection under the terms of the service level agreement.
3. The RSN Acceptable Use Policy applies in the first instance to any organisation authorised to use RSN (a **"User Organisation"**). It applies also to use of RSN by the User Organisation's own members and all those to whom it otherwise provides with access to RSN (collectively, its **"Members"**).
4. It is therefore recommended that each User Organisation establishes its own statement of acceptable use within the context of the services provided to its Members, and in a form that is compatible with the conditions expressed in the RSN Acceptable Use Policy. Such a statement may refer to, or include, this document. If material from this document is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of the RSN Acceptable Use Policy. The EDIT Team Help Desk can advise on this aspect as and where necessary.
5. Those implementing this RSN Acceptable Use Policy within a User Organisation should also take into account the provisions of the *RSN Security Policy* and associated guidance documents, in respect both of the connection of IT systems to RSN via the User Organisation's network and of individual Members' access to RSN.
6. Copies of the RSN Service Level Agreement (**"SLA"**) Terms, and of the RSN Security Policies may be found on the Rochdale Schools Intranet, via the URLs given alongside other RSN contact details at the end of this document.

Acceptable Use

7. A User Organisation and its Members may use RSN for the purpose of communicating with other User Organisations and their Members, and with organisations, individuals and services attached to networks which are reachable via RSN. All use of RSN is subject to the RSN SLA Terms.
8. Subject to clauses 10 to 18 below, RSN may be used by a User Organisation and its Members for any lawful activity that is in furtherance of the aims and policies of the User Organisation.
9. It is the responsibility of the User Organisation to ensure that its Members use RSN services in accordance with this RSN Acceptable Use Policy, and with current legislation.

Unacceptable Use

10. RSN may not be used by a User Organisation or its Members for any of the activities described below.
11. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

12. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
13. Creation or transmission of material with the intent to defraud.
14. Creation or transmission of defamatory material.
15. Creation or transmission of material such that this infringes the copyright of another person.
16. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.
17. Deliberate unauthorised access to networked facilities or services.
18. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
 - a. wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems;
 - b. corrupting or destroying other users' data;
 - c. violating the privacy of other users;
 - d. disrupting the work of other users;
 - e. denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment);
 - f. continuing to use an item of networking software or hardware after RSN has requested that use cease because it is causing disruption to the correct functioning of RSN;
 - g. other misuse of RSN or networked resources, such as the introduction of "viruses" or other harmful software via RSN.

Access to Other Networks via RSN

19. Where RSN is being used to access another network, any breach of the acceptable use policy of that network will be regarded as unacceptable use of RSN. Any deliberate activity as described in clause 18 above, and where applied to a user of that network, will also be regarded as unacceptable use of RSN.
20. Any breach of industry good practice (as represented by the standards of the London Internet Exchange) that is likely to damage the reputation of the RSN network will also be regarded *prima facie* as unacceptable use of RSN.

Passing on and Resale of RSN

21. A User Organisation may extend RSN access to other individuals on a limited basis where this is done in pursuance of the User Organisation's remit and for which it receives public funds, provided no charge is made for such access.
22. It is expected that such use will be regulated by the User Organisation in the same manner as it would regulate occasional use by third parties of its other facilities, such as its telephone and IT support systems. Any individual using RSN in this manner must therefore be subject to the same requirement to use RSN in an acceptable manner as is required by the User Organisation of its Members.
23. Otherwise, a User Organisation is not permitted to provide access to RSN to third parties without the prior agreement of the Impact Partnership (Education IT Services) – EDIT Team.
24. This agreement will normally take the form of licensing by RSN of the User Organisation to provide such access. Details of such licensing schemes are available from the EDIT Team upon request.

Compliance

25. It is the responsibility of the User Organisation to take reasonable steps to ensure its Members'

compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of RSN is dealt with promptly and effectively should it occur. The discharge of this responsibility

includes informing all Members of the User Organisation with access to RSN of their obligations in this respect.

26. Where necessary, service may be withdrawn from the User Organisation, in accordance with the RSN SLA Terms. Where violation of these conditions is unlawful, or results in loss or damage to the Impact Partnership (Rochdale Borough) Ltd. or EDIT Team or RSN resources or the resources of third parties accessible via RSN, the matter may be referred for legal action.

Appendix 9 - RSN 'Passwords'



RSN Password Policy

1. Purpose

The purpose of this document is to outline the minimum requirements for passwords used on the Rochdale Schools Network (RSN) by its registered users and predefined systems. It will outline how they are to be created and give advice for schools and staff on choosing memorable and secure passwords (see Appendix 1) as well as the responsibilities of RSN users in protecting and safeguarding credentials.

2. Use of Passwords

Passwords are used to restrict access to systems and ensure that only registered and permissions individuals have used of them. It is the responsibility of each individual not to disclose their own personal password credentials to another individual and to change it if they suspect that it has been compromised.

Similarly users must not disclose generic username and password credentials, where used, to individuals outside of their own educational establishment.

Passwords should not be written down or stored near to workstations or devices that can access RSN. The **only exception** to this is where generic pupil credentials are required to be displayed for ease of class management.

3. Minimum Requirements

- 3.1 All user account passwords should contain
- a minimum of eight (8) characters
 - at least one (1) lowercase letter
 - at least one (1) uppercase letter
 - at least one (1) number.

3.2 All system account passwords should also contain

- at least one (1) symbol !?£&@-#%^*+=_<>\$[]{}() or space

4. Defaults

4.1 By default, generic and individual student accounts will be set to

- never expire
- not allow user to change password

4.2 By default, individual staff accounts will be set to

- expire after ninety (90) days
- allow user to change password
- allow user to reuse previously chosen password

4.3 By default, system account will be set to

- never expire
- allow user to change password
- not allow user to reuse previous ten (10) chosen passwords

5. Setting and Changing Passwords

5.1 Individual Staff Accounts

A password will be reset for an individual via the helpdesk only by direct request of the individual. All passwords will be reset to Password123 and require that the user changes the password at next login. This will ensure that only the individual involved will know their final chosen password. Users may reset their own password by doing Ctrl + Alt + Delete and choosing Change Password. They must submit their existing password and retype their chosen new password twice ensuring it complies with the minimum requirements outlined in 3 above.

Initial user credentials, including password details will be sent to the school's office@ e-mail address for distribution to the relevant member of staff. Initial password will be Password123 and Require that the user changes the password at next login. This will ensure that only the individual will know their final chosen password.

5.2 Generic and Individual Student Accounts

Requests to change generic accounts must be submitted via the relevant form on the Rochdale Schools Intranet (RSI). Submitted requests are verified via e-mail with the headteacher of the school before being processed to ensure the submitted changes are satisfactory unless submitted by the headteacher of the school, in which case they are processed automatically.

Schools are only allowed to change their generic passwords once a term unless there are specific special circumstances.

5.3 System Accounts

These will be changed whenever a member of technical staff who has had access to these accounts leaves their employment.

Defined: July 2012

Review: January 2014

Appendix 1: Setting a Memorable Password

1. Car Registration

Change certain letters for numbers or symbols, ie.

A = 4 or @	B = 8	H =	N = ^	O = 0	T = +
		#			
C = (or <			P = 9		Z = 2 or ~
E = 3 or £ or =		I = 1 or ! or	J = ?	R = /	
6 or &		K =		S = 5 or \$	
		%	L		
		=	7		

Therefore a memorable eight letter word like elephant could become E73p#@nt

2. Sentences and text speech

Use the first letters of each word from a memorable sentence and/or text speech, ie. "I like to

-- --

eat fish and chips on Friday" could become Il2efacoF

Appendix 10 – RSN ‘Security’



RSN **Security Policy**

December 2009

Background

1. It is the aim of RSN, as a network for primary, nursery and special educational needs, it will be most effective if it places as few technical restrictions as possible on the use of new applications and

services. The imposition of mandatory access control or monitoring systems is likely to cause problems for existing uses of the network as well as limiting future developments, and should only be considered where there is a clear benefit. Filtered or restricted network access is mandatory in order to comply with Safeguarding and Child Protection Legislation, however the core RSN service should provide as open a network as is possible while meeting operational and legal requirements.

2. A presumption of openness brings associated risks that security incidents or misuse will seriously damage the effectiveness of the network (a summary of these risks can be found in Annex A). The impact of incidents may rapidly spread far beyond the individual organisation, machine or user where they originate. These risks must be managed if the network is to fulfil its purpose. The RSN has therefore adopted this Security Policy to protect the network and the organisations that use it. Under the Terms for the Provision of the RSN Service, compliance with this Policy is a requirement for all organisations connected to the network. The Policy also places responsibilities on users of the network. The authority of EDIT, The Impact Partnership as service provider, to protect the operation of the network is established in the Terms for the Provision of the RSN Service.
3. This RSN Security Policy therefore has a number of goals:
 - To ensure that appropriate local policies exist to protect RSN, the networks connected to RSN and the computer systems using RSN from abuse (whether defined in this or other RSN Policies);
 - To ensure that mechanisms exist to aid the prevention and identification of abuse of the RSN network;
 - To ensure an effective response to complaints and queries about real or perceived abuses of the RSN network;
 - To ensure that the reputation of RSN is protected and that the network can meet its legal and ethical responsibilities with regard to its connectivity to the worldwide Internet.

Definitions

4. The term RSN refers to the Rochdale Schools Network and all associated centralised services.
5. The term 'Connected Organisation' means any organisation with a connection to the RSN network, this typically is a primary, nursery or special school.

The Policy

Responsibilities

6. The Terms for the Provision of the RSN Service place responsibilities on every person and organisation involved in the use or operation of RSN to protect the network against security breaches. In particular:
 - Each Connected Organisation must ensure that all use of RSN by those individuals and groups to whom it provides network access complies with this Security Policy and the RSN Acceptable Use Policy. The Connected Organisation must also ensure that information about security issues can be communicated rapidly within the organisation and to EDIT, The Impact Partnership and that problems are resolved promptly (see paragraphs 7 and 8);
 - Each Connected Organisation must ensure that its actions and those of the users for which it is responsible are safe for themselves and do not present a threat to others (see paragraph 9);
 - Each user of the RSN network and the networks of Connected Organisations must behave in accordance with this Security Policy and with any policies and procedures local to the Connected Organisation. The user must cooperate with their organisation and the network operators to reduce security risks;
 - EDIT, The Impact Partnership must ensure that the operation of the network is appropriately monitored, that the response to security problems is coordinated, and that temporary or permanent measures are implemented, up to and including disconnection, where necessary to protect the network or to comply with the law (see paragraph 10).

Points of Contact at the Connected Organisation

7. The successful prevention of security incidents and prompt resolution of those that do occur both depend critically on the rapid and accurate transfer of information between RSN Connected Organisations and EDIT, The Impact Partnership as operator of the network. To this end each Connected Organisation must provide EDIT, The Impact Partnership with up-to-date details of one or more persons who will act as Security Contact(s) for the Connected Organisation and any other organisations and individuals to whom the Connected Organisation provides access to RSN. The Connected Organisation must ensure that its designated Security Contact(s) have appropriate authority to fulfil their role (see **note 1**).
8. The Security Contact(s) have roles in both the prevention and resolution of security incidents:
 - To disseminate EDIT, The Impact Partnership's warnings of general risks and precautions to appropriate people within the organisation(s) for which they are responsible, and to ensure that appropriate preventive measures are taken promptly;
 - To ensure that any particular security breach or risk that has been reported to the Security Contact(s) by EDIT, The Impact Partnership as affecting an organisation for which they are responsible is investigated and resolved promptly, and to inform EDIT, The Impact Partnership that this has been done.

Responsible Action by the Connected Organisation

9. Each Connected Organisation must act responsibly to protect the network. This duty includes:
 - Taking effective measures to ensure that there is no security threat to RSN or other Connected Organisations from insecure devices connected to the Organisation's network (see **note 2**);
 - Taking effective measures to protect against security breaches, in particular ensuring that recommended security measures are implemented;
 - Taking effective measures to ensure that security breaches can be investigated and that other users of the network are protected from the consequences of breaches;

- Assisting in the investigation and repair of any breach of security; Promoting local policies in support of this RSN Security Policy, backed by adequate disciplinary and other procedures for enforcement;

- Implementing appropriate measures for giving, controlling and accounting for access to RSN, backed by regular assessments of the risks associated with the measures chosen (see **note 3**);
- Taking reasonable measures to encourage its users to act responsibly in compliance with this Policy and the RSN AUP, and ensuring that they are enabled to do so through systems, procedures and training that support good security practice.

Monitoring and Enforcement by EDIT, THE IMPACT PARTNERSHIP

10. The Terms for the Provision of the RSN Service authorise EDIT, The Impact Partnership, as the service provider responsible for the RSN network, to require connected organisations to comply with this Policy, to monitor the network where it has reason to believe there has been a breach of the Policy or other threat, and to take such actions as are necessary to protect the operation of the network and the security of services provided to RSN customers (see **note 4**).

In particular EDIT, The Impact Partnership is authorised to:

- Monitor use of the network, while respecting privacy and national law, either in response to information about a specific threat or generally because of the perceived situation;
- Implement such temporary technical measures as are required to protect the network or its customers against breaches of security or other incidents that may damage the network's service or reputation;
- Require a Connected Organisation, through its nominated contact, to fulfil its responsibilities under any of the RSN Policies;
- Where a Connected Organisation is unable or unwilling to co-operate, initiate the process for achieving an emergency disconnection;
- Where permitted or required by law, assist law enforcement authorities in their investigations concerning the RSN network.

Explanatory Notes

1. Further details of the role of the Security Contact can be found in the Technical Support area on the Rochdale Schools Intranet. Typically the Security Contact is the Head Teacher or member of the Senior Leadership and Management Team and possibly the IT Coordinator.
2. The security of networked devices may, for example, be managed by a combination of direct configuration and maintenance, technical controls such as firewalls or router access control lists, system monitoring or probing, and delegation to appropriately skilled others. Where an organisation allows a device it does not own or control to connect to the network it is strongly recommended that consent to these normal operational measures be obtained as a condition of connection.
3. Further information about granting and accounting for access can be found in the factsheet 'User Authentication' on the Rochdale Schools Intranet.
4. On occasion, RMBC may assist in the investigation of misuse or protection of the network under their contracts with The Impact Partnership.

Annex: Risks to Networks and Networked Systems

All computer networks are exposed to threats, both internally and from the other networks to which they connect. Hostile traffic, both random and directed, is now a constant feature of the Internet. The particular open character of an education network (albeit in a walled-garden setting) increases both its exposure to these threats and the potential damage to the integrity and effectiveness of the network. The risks to the network, the computers and organisations connected to it, include:

- **Breaches of confidentiality.**

Organisations hold and have access to large amounts of intellectual property, both their own and licensed from others: the value of such property may be greatly reduced if it is disclosed to others. Organisations also handle a great deal of personal information about individuals who may suffer if it is not kept confidential: consequences range from a loss of privacy to partial or complete theft of identity.

- **Loss of integrity.**

Information held on computers can be destroyed or modified, and unauthorised changes may be undetectable. The integrity of computers themselves may be compromised if intruders are able to take control of them, thus casting doubt on the accuracy of any results and the privacy of any data. Repeated failures can result in users losing confidence in computer systems at their own or other organisations.

- **Failures of availability.**

Networks and the computers connected to them may be temporarily disabled either deliberately or accidentally by large flows of network traffic, making them unusable at critical times. Organisations that lose the confidence of others may find themselves unable to communicate if they are placed in a blacklist. Network and computer staff may be unavailable for support or development activities if they have to spend their time dealing with security incidents.

- **Damage to reputation.**

The reputations of RSN and the organisations and individuals connected to it may be seriously harmed by security incidents or inappropriate use of the network. Many intruders like to advertise their successes, others may attack third parties using computers connected to RSN and to which they have gained control. Organisations whose systems are used in these ways are likely to be

held responsible. The use of RSN to disseminate unwanted, offensive or illegal material is also likely to be seen as misuse of a publicly-funded resource.

- **Legal action.**

National and international law is increasingly concerned with data networks and is placing a growing list of obligations on those who provide them. Individuals, organisations and network operators who, by action or inaction, fail to meet their legal obligations may be punished by the criminal law, have substantial financial damages awarded against them or be required to modify or cease their networking operations.

The openness of RSN and other connected networks may allow the impact of a security breach to spread far beyond an original insecure system or action. The same openness means that it will rarely be possible to protect organisations and users against the immediate consequences of their insecure actions: more often it will be necessary to respond promptly to security breaches by isolating the systems and organisations affected until the problem has been resolved.

Appendix 11 - RSN 'Approved Software & Use of Portable Storage Devices'



RSN

Approved Software and Use of Portable Storage Devices Policy

1. Approved Software

Unlicensed or personal software must not be installed on the School's hardware, or connected in any way to the School's equipment or systems. If software is deemed to be of use to the School then it should be duly acquired by the School under licence.

2. Use of Portable Storage

Use of the portable media (floppy disks, CD's, pen-drives, etc) on networked PCs is not permitted unless recorded authorisation has been given by School management. **Where authorisation has been given to a specific user it is his/her responsibility to ensure that all inserted media do not transmit any viruses onto**

the School's network. Devices which have been used on other PCs, networked or otherwise, within or outside the School must not in any case be used on PCs connected to the School's network until the disks have been checked through appropriate and agreed virus checking procedures. In particular it is recommended that pupils refrain from using such media unattended and school staff monitor usage of any devices or drives that may be required in line with good practice outlined above.

3. Contact Point Workstation Approved Software

The following titles/generic products are currently listed as approved software for installation on Windows Workstations set to use Contact Point. Items not on this list should be installed until testing has been undertaken by authorised technicians.

Microsoft Office 2003 Professional Applications upwards

- Microsoft Office Excel 2003
- Microsoft Office FrontPage 2003
- Microsoft Office Outlook 2003
- Microsoft Office PowerPoint 2003
- Microsoft Office Word 2003

Windows OS Updates and Patches

- Windows Genuine Advantage
- Windows Hotfixes
- Windows Installer 3.1 upwards
- Windows Security Updates
- Windows Service Packs

Printer Driver Applications

- Dell Solution Centre
- Dell Printers
- HP Help & Support
- HP Printers
- OKI LPR Utility
- OKI Network Extension
- Ricoh Printers
- Sierra Print Artist 4.0
- Sierra Utilities

Security and Protection

- Microsoft AntiSpyware

-
- Sophos AntiVirus
 - Spybot - Search & Destroy 1.3 upwards
 - Windows Defender

Terminal Hardware Applications

- Broadcom Advanced Control Suite
- Broadcom ASF Management Applications
- Broadcom Management Programs
- Easy CD Creator 5 upwards
- HighMAT Extension to Microsoft Windows XP CD Writing Wizard
- Intel® drivers and applications
- InterVideo WinDVD
- Microsoft IntelliPoint
- Microsoft IntelliType
- SoundMAX

Utilities

- Adobe Acrobat
- Adobe Reader
- J2SE Runtime Environment 5.0 upwards
- Java 2 Runtime Environment, SE v1.4.2 upwards
- Macromedia Flash Player
- Macromedia Shockwave Player
- Microsoft Framework 1.1 onwards
- Microsoft Internet Explorer
- Microsoft Windows Journal Viewer
- Microsoft XML Parser
- MSXML 4.0 SP2 Parser and SDK
- QuickTime
- RealPlayer
- Shockwave
- User Profile Hive Cleanup Service
- WebFldrs XP (v9.50.5318)
- Windows Media Connect
- Windows Media Format Runtime
- Windows Media Player 10
- WinVNC 3.3.2
- WinZip v.8 upwards

Miscellaneous

- Desktop Publisher
 - eProfile
 - GraphicView 32
 - IEPWriter
 - OSMIS Framework
 - Pupil Achievement Tracker
 - SIMS Infrastructure
 - ypoOrder
-

Appendix 12 – RSN ‘Data Handling Procedures & Guidelines’



RSN

Data Handling Procedures and Guidelines

1. All staff will be issued with ID cards which must be worn at all times and challenge people that are not wearing them.
2. Staff will record all visitors to buildings and wherever feasible ensure that they are accompanied whilst on the premises.
3. Staff will implement a clear desk/clear screen policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when areas are unattended.
4. Staff will ensure where personal information is held on paper, it is locked away when not in use or the premises are secured.
5. All personal information should be securely destroyed: paper records by incineration, pulping or shredding so that reconstruction is unlikely and electronic media by overwriting, erasure or degaussing for reuse.
6. Wherever possible the use of removable media including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats should be avoided. Where it is unavoidable, encryption **must** be used and the information transferred should be the minimum necessary to achieve the business objective.
7. Access to systems should be restricted to those users that need it. This will be achieved through Active Directory Group Policy and file/folder permissions. Access to raw data will be strictly controlled and only anonymous data should be readily available.
8. Where it is not possible to access information on secure premises and systems, the following hierarchy should apply:
 - a. Access should be via secure remote access so that information can be viewed or amended without being permanently stored on the remote computer.
 - b. Next best is secure transfer of information to a remote computer on a secure site on which it will be permanently stored.
 - c. Decisions on handling/transfer of information should be approved in writing by the relevant information asset owner.
 - d. User rights to transfer information to removable media should be carefully considered and strictly limited. Where it is necessary to bulk transfer information, it should be done electronically across the secure network.
9. Where information needs to be shared between organisations secure networks must be used. It is never acceptable to transfer bulk personal information via normal e-mail services. The use of the Rochdale Schools Intranet should be utilised to assist in the communication between RMBC, RSN and Secondary School systems.

10. Review

Appendix 13 – Smithy Bridge ‘Privacy Notice 2014-15’

Schools Privacy Notice - 2014/2015

Data Protection Act 1998

We, Smithy Bridge Primary School are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data to:

- Support your learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well we are doing.

Information about you that we hold includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs you may have and relevant medical information. If you are enrolling for post 14 qualifications the Learning Records Service will give us your unique learner number (ULN) and may also give us details about your learning or qualifications.

We are required by law to pass some information about that we hold about pupils and parents to the Local Authority and the Department for Education (DfE). The Local Authority may occasionally be required to share your personal and sensitive information with other government and/or partner agencies. The Local Authority will only share data when there is a statutory duty or legal requirement to do so, for example, where the Local Authority is required to provide a programme of assistance. Any data that the LA share with government and/or partner agencies will be strictly assessed and the Local Authority will ensure that the requirements of the Data Protection Act 1998 are complied with.

If you want to receive a copy of the information about you that we hold or share, please contact **the school office**.

If you need more information about how the Local Authority and DfE store and use your information, then please go to the following websites:

http://www.rochdale.gov.uk/council_and_democracy/data_protection_and_foi/pupil_data.asp
[x](#)

Information Governance Unit
Rochdale Council
Number One Riverside, Floor 2
Smith Street
Rochdale
OL16 1XU

Email: foi@rochdale.gov.uk
Telephone: 01706 925505

or

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT

Email: <http://www.education.gov.uk/help/contactus>

Telephone: 0370 000 2288

Appendix 14 – RSN ‘Backup’



Based on Becta
Framework for ICT Technical Support OM (FITS OM)
Storage Management

Backup Policy – School-based File Stores

The following information is designed to help users of the Rochdale Schools Network understand the nature of the ICT backup procedures and the availability of information beyond the date on which users delete it.

The back up of files from each school primary server is for the purpose of ensuring schools' ability to recover from computer or network failures or disturbances. The ICT backup system is not designed or intended to be a means for members of the school community to have access to long-term storage of files.

We run backups of the key school systems daily, usually starting anytime between 9.00pm and 3.00am finishing a couple of hours after that. Certain systems or disks may be backed up earlier and/or take longer to finish.

Each daily backup saves the contents of identified files and directories at the time the backup takes place. Therefore the backups do not record all activities or all contents of users' files throughout the day or week: a backup is simply a snapshot of the data present on the system at the time the backup ran. This means that during the course of a day it is possible for a user to create and delete a file which will never appear on a backup.

We retain full backups of key central school admin, teaching files and MIS information every month and do incremental backups for 60 working days following this, so we can retrieve daily backups for up to 60 consecutive working days before the date of request. In addition a full backup of centrally stored monthly full backups are done every quarter and stored off-site from the main remote storage facility. Users are urged to back up any critical information themselves for archival purposes or long-term storage offline.

Key school admin files are defined as those related to personnel, finance and policies usually stored on the Admin network drive or P: drive and Staff drive or O: drive. Teaching files are defined as those required for the delivery of the curriculum such as planning, assessments, SEN pupil related reports and other teaching related administrative files but do not include media content such as images, video or sound. These are usually stored on the Staff network drive or O: drive. MIS information is defined as the data related to the schools management information system.

Primary servers have a minimum of three forms of backup – networked RAID 1, networked attached storage (NAS), and local removable disc storage.

RAID 1 (Redundant Array of Inexpensive Disks) is a method which spreads information is spread across several disks to achieve redundancy, lower latency and/or higher bandwidth for reading and/or writing and to facilitate recoverability from hard-disk crashes. These are located in secured environments within the Rochdale Local Authority and operate via the Wide Area Network (WAN).

Schools have the option to use onsite removable storage media to run full backups of data stored on their system. This can be in the form of removable data cartridges from a device built into the school server or from a separate NAS device which allows the flexibility to connect to the internal school network from any location within the school site (where wired network access is available) and has the capacity to retain more data. Schools are recommended to do a minimum of a full backup each month and year using the removal disk media recommended. The most recent monthly and annual full backups should be transferred offsite and stored in a safe. A full backup is defined as a snapshot of the data needed for carrying out normal school business and may not include trivial data stored on some drives or data stored on local workstations.

Appendix 1: Defined Paths

The following folders will be included in the backup of each school server. The contents of these folders will be backed up and should be populated with relevant files.

Assessment document O:\Assessment

Finance documents: P:\Finance and P:\Pastel

Personnel documents: P:\Personnel

Planning documents O:\Planning

Policy documents: P:\Policy and O:\Policy SEN

documents (IEP etc). O:\SEN

And all MIS related information from SIMs.NET (attendance, behaviour, assessment, document storage)

Appendix 2: Verification

As part of the backup process testing will take place to ensure recovery of information is possible. This will be done using a random sample of data backed up and to a test environment. Any files recovered will be deleted from the test environment following the verification process.

Appendix 3: Incorrect Files

If during this process it is discovered that schools have incorrectly placed files into these folders that do not appear to meet the key business critical data definitions as stated above then the school will be contacted and asked to relocate these files elsewhere on their school server to be backed up using on-site school based backup solutions. This is to maintain a fair process for all schools using the system. Failure to comply with this request within 3 working days will result in the suspension of

the offline backup facility until the matter is resolved. School will be notified should this action be taken.

Appendix 15 – RSN ‘Backup & Disaster Recovery’

RSN: Backup and Disaster Recovery Information & Advice

Purpose

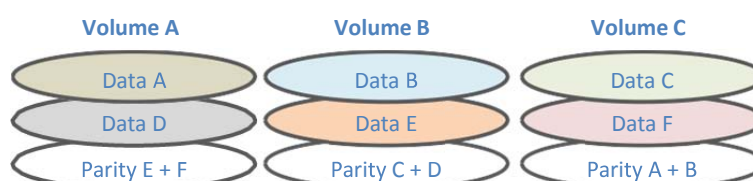
The purpose of this document is to provide a summary of the current backup and disaster recovery solutions in place within the Rochdale Schools Network and make recommendation for schools to further enhance and supplement the current provision in the event of complete system failure. Schools are recommended to act following reading this document.

Background

Currently all data held on the school server is set in a RAID 5 array. This means that all the discs within the server are combined and then sub-divided into volumes of data. These volumes are set up such that data is interleaved across all physical hard-drives with parity data calculated and stored in a separate volume so that the data can be recovered (see diagram below). This allows for the safe replacement of faulty discs whilst retaining data integrity.



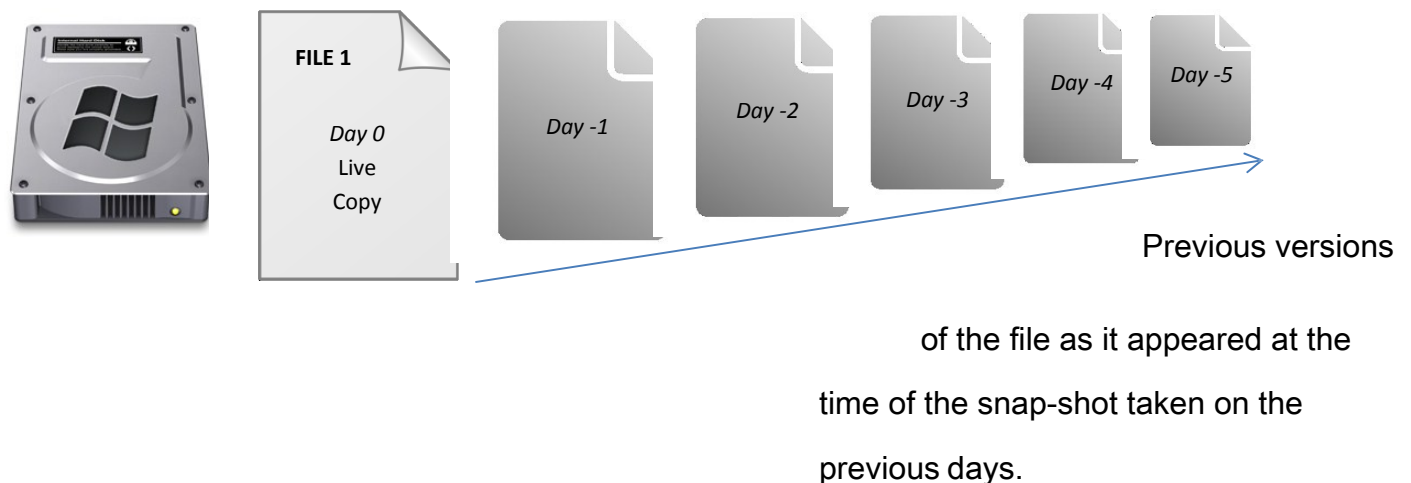
Example



Additionally, across the hard-drives, shadow copy is enabled. This means that each and every file has a history attached to it of around 2-3 weeks (depending on the total amount of data held) such that a ‘previous version’ of any file could be applied if needed. ‘Previous version’ refers to the state of the file at the time the snapshot was taken.

Therefore if a snap shot was taken on day X at 09:00 and changes were made to the file throughout the day and the file was subsequently accidentally deleted later that same day, the

restored file from the previous version would be as it was at 09:00 on that day without the subsequent changes made to it throughout that day.



At the same time an incremental copy of a subset of these files are kept off-site on centralised servers as defined by the current backup policy as ‘key critical data’ identified by Becta in their 2009 publication on the recommendations for school backups. This currently covers the following specific folder and their contents:

O:\Assessment	Assessment document
O:\Planning	Planning documents
O:\SEN	SEN documents
(IEP etc) P:\Finance and P:\Pastel	Finance documents
P:\Personnel	Personnel
documents P:\Policy and O:\Policy	Policy
documents	
S:\SIMS	All MIS related information from SIMs.NET (attendance, behaviour, assessment, document storage and discover)

This off-site incremental copy allows restoration for up to 60 days using Microsoft Data Protection Manager (DPM). We have limited the remote backup to this subset of data due to limitations of storing data for this length of time and that of bandwidth on the physical connections between schools and the data-centre. If all schools wished to back-up all content every day we would have to increase the bandwidth and the storage capacity. This in turn would have a knock-on effect on the cost to schools and the ability for this service to be delivered in a manageable way.

Disaster Recovery

Currently there is no solution for a complete system failure in the unlikely event where all RAID disks fail in a server. To this end we are currently recommending schools invest in one of the following solutions to enable a disaster recovery copy of all the school's server data to be held. This copy is intended for the purposes of complete system failure and recovery of the system in such an event and not for the purposes of day-to-day backup and recovery of individual files or folders; the existing processes and procedures already in place should adequately allow the safe recovery of such files either through shadow-copy restoration or DPM.

Option

1.



Summary: Purchase, install and configure Weston digital 4 TB encrypted USB hard drive to provide a snapshot backup each day at 18:00.

Operation: School to manage fitting of USB device to server on a daily, weekly, monthly or termly basis. If they choose to have **multiple** USB drives they would be responsible for switching the devices at agreed times. We would recommend at least once a week, ie if the school bought two (2) USB drives they would alternate them between week A and week B with the USB drive not being used stored in a safe location away from the server. This would be our minimum recommendation.

The 'backup' will be a simple snap-shot of the current server data at the time of the backup.

Support: This option is seen as a self-supporting solution following initial configuration. If schools buy in technical support this could be one of the duties of the technician on site during their visit. Recovery of data would take place only if total disc failure occurs on the main server and there is a need for a copy of the 'latest' data held.

Cost: £180 per USB plus installation and configuration at standard rates.

From Stone Computers, order:

STOHAR-736 Western Digital My Book Studio 4TB Ext Hard drive USB3 PC and MAC 1

Option 2: NAS

Summary: Purchase, install and configure Weston digital sentinel 8 TB (RAID) NAS box to provide a snapshot backup each day at 18:00.

Operation: The NAS box would be located in a different location from the school server somewhere within the school. The NAS box would be a managed device on the network which can be accessed locally or remotely. The NAS box could hold multiple copies of the main server (at least 2) which would give the school and technicians options should the data

become corrupted and/or there is a main-disc failure on the main server.

The 'backup' will be a simple snap-shot of the current server data at the time of the backup.



Support: This is seen as a self-sustained solution following initial configuration. Recovery of data would take place only if total disc failure occurs on the main server and there is a need for a copy of the 'latest' data held.

Cost: £895 plus network cabling costs (if required) and installation and configuration at standard rates.

From Stone Computers, order:

WESTERN DIGITAL WD Sentinel DX4000 8TB including Guardian Pro for Sentinel - 3 Year Warranty

Option 3: Custom Bespoke Solution

Summary: Our technical staff would work with the school to create a custom solution to fit the school's requirements; this could include tape drives, a NAS Box with synchronized cloud storage or a combination of solutions.

Operation: dependent on solution but we would assume that this may be a managed solution

Support: dependent on solution but would assume that EDIT manage this on behalf of the school OR the school manage it themselves following initial install and configuration. There would be different pricing models for these two options, dependent on the final solution chosen.

Cost: dependent on requirements and final solution chosen. There will be a minimum cost of 1 day (charged at standard rates) for the initial consultation (visit and producing options) required for this work.

Potential costs for elements of a system that *might* be considered, but not limited to, are;

STOHAR-736 Western Digital My Book Studio 4TB Ext Hard drive USB3 PC and MAC1	£180.00
WESTERN DIGITAL WD Sentinel DX4000 8TB including Guardian Pro for Sentinel	£895.00
TAPE DRIVE LTO-6 2500GB/6125GB Table Top Bundle	£1,975.0
Dropbox (unlimited storage pa per user)	£463.00 pa
ZEN internet (up to 200Gb storage allowance)	£2,759.40 pa
Redstor Virtual DR	£custom
Redstor Backup for Schools	£custom

Should schools require an archiving solution we would recommend using Option 1 and storing either a subset of the schools data (ie. that which requires archiving) or the whole server to be archived on the portable USB drive and then stored in a safe and secure location, preferably off-site.

School Actions

Schools should choose to adopt one of the three options recommended above or make their own arrangements. Schools should order the equipment required direct from the supplier (Options 1 and 2) and book an appointment for the work to be completed by logging a service request via the helpdesk. Should schools choose Option 3 they should book an appointment for the initial consultation to take place via the helpdesk. In both cases someone will contact the school to arrange a suitable date and time.

Definitions:

<i>Archive</i>	a copy of data held which is stored for a pre-defined time as dictated by policy or legislation and used for the purposes of reference and fact finding at a later date
<i>Backup</i>	a procedure for copying data or subset of data in a secure manner such that it can be recovered due to loss of data or equipment
<i>Disaster Recovery (DR)</i>	procedures and processes to recover an entire system should it catastrophically fail, be lost or destroyed
<i>Incremental</i>	a term used in backup processes to compare existing backup data with the currently held live data and only copying differences between the two to the backup version.
<i>NAS</i>	Network Attached Storage, a device attached to the network via fixed network cabling used as additional storage for a local area network
<i>RAID</i>	Redundant Array of Independent Disks, several hard disks are made into one logical disk. The main reasons why RAID is used are (i) to make the loss of data happen less often. This is done by having several copies of the data, (ii) to get more storage space by having many smaller disks, (iii) to get more flexibility (disks can be changed or added while the system keeps running) and (iv) to get the data more quickly.
<i>USB</i>	Universal Serial Bus, an input/output on a workstation or server to connect additional devices and peripherals so they can interact with operating system on the computer

LAN Local Area Network, the interconnection of workstations and servers by network cabling and switches so that devices can communicate with each other and share data and resources

Shadow Copy a technique used by the operating system of a computer to make a copy of all files on its system so that these previous versions can be reinstated should loss or unintended alterations be made to individual files or folders

Volume An allocation of storage that is less than or more than one physical drive. For RAID 5 the volume set spans several physical drives but the operating system see the volume set as a contiguous group of storage blocks even though the physical data resides on multiple drives.

Disclaimer

All prices for equipment quoted in this guidance are correct and based on best-value quote obtained from several companies at the time of publication. Other suppliers offer the same equipment and schools may be able to achieve better value-for-money elsewhere. Schools should use their own procurement rules in ascertaining best-value. Our current recommendation is for Western Digital appliances.



Smithy Bridge Primary School

Social Networking Policy

Introduction to the Policy

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The two with the widest use are Facebook and MSN. The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation. This policy and associated guidance is to protect staff and advise school leadership on how to deal with potential inappropriate use of social networking sites. The policy requirements in this document aim to provide this balance - to support innovation whilst providing a framework of good practice.

Purpose

The purpose of this policy is to ensure:

- That the school is not exposed to legal risks
-

-
- That the reputation of the school is not adversely affected
 - That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

Facebook is targeted at older teenagers and adults. They have a no under 13 registration policy and recommend parental guidance for 13 to 16 year olds.

The following are extracts from Facebook privacy policy:

"If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us"

"We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices. Materials to help parents talk to their children about safe internet use can be found on this help page"

MSN recommend 13 but do not appear to have a policy of debarring younger pupils.

There are many primary age pupils active on MSN.

This guidance is to advise and protect staff from accusations of improper relationships with pupils:

SCOPE

This policy covers the use of social networking applications by all school stakeholders, including, employees, Governors and pupils. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this policy apply to all uses of social networking applications which are used for any school related purpose and regardless of whether the School representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:

- Blogs, for example Blogger
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media sharing services, for example YouTube
- 'Micro-blogging' applications, for example Twitter

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Use of Social networking sites in work time

Use of social networking applications in work time for personal use is not permitted, unless permission has been given by the Head Teacher.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first.

Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head teacher. However, school representatives must still operate in line with the requirements set out within the policy

School representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all school representatives.

This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Smithy Bridge Primary School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Terms of Use

Social Networking applications

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/protection for staff on using social networking

- No member of staff should interact with any pupil in the school on social networking sites
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the head teacher in writing. However, it would not be appropriate to network during the working day on school equipment
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection person in school

Guidance/protection for Pupils on using social networking

- No pupil under 13 should be accessing social networking sites. This is the guidance from both Facebook and MSN. There is a mechanism on Facebook where pupils can be
-

reported via the Help screen; at the time of writing this policy the direct link for this is:

http://www.facebook.com/help/contact.php?show_form=underage

- No pupil may access social networking sites during the school working day
- All mobile phones must be handed into the KS2 staff at the beginning of the school day, the Internet capability must be switched off. Failure to follow this guidance will result in a total ban for the pupil using a mobile phone
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens
- No school computers are to be used to access social networking sites at any time of day.
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision
- Please report any improper contact or cyber bullying to your class teacher in confidence as soon as it happens.

Child protection guidance

If the head teacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they should:

Record the disclosure in line with their child protection policy

Schools must refer the matter to the LADO

If the disclosure has come from a parent, take normal steps to calm the parent and explain processes

If disclosure comes from a member of staff, try to maintain confidentiality

The LADO will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.

If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out

Cyber Bullying

By adopting the recommended no use of social networking sites on school premises, Smithy Bridge Primary School protects themselves from accusations of complicity in any cyber bullying through the provision of access.

Parents should be clearly aware of the school's policy of access to social networking sites.

Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

This can be a complex area, and these examples might help:

A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.

A child is receiving taunts from peers. It is all at weekends using MSN and Facebook.

The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.

A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5: This is the tricky one. The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the schools

recommendation. They could then deal with residual bullying in the school, but refuse to deal with the social networking issues.

If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment

This guidance can also apply to text and mobile phone cyber bullying.

Appendix 17 - 'Policy for Employee Use of E-mail, Internet, Mobiles & Intranet

Smithy Bridge Primary

Policy for Employee use of E-mail, the Internet, Personal Mobile Phones and Rochdale's Intranet

1. General Policy Statement

This policy applies to all employees, trainee teachers, students on placements and other volunteers within the school, whatever their employment status, and to all school desktop and portable computers, portable memory etc, whether they are located on school premises or at other locations, and to personal mobile phones that are brought onto school premises. It also applies to employees who have access to the school system from home or whilst off site on school business. (IT security is viewed seriously by the school and any breach of this policy could lead to disciplinary action being taken against those who commit this breach. Serious violations will be considered gross misconduct and as such may lead to the dismissal of the employee(s).)

2. Objectives of the policy

This document sets down the school's policy on the use of school telephones, e-mail system and the Internet within work. It is important that you read the policy carefully as the school requires compliance from all employees, trainee teachers, students on placements and other volunteers at all times.

The policy has been devised to enable both the school and its employees to gain maximum benefit from e-mail and Internet, to protect the school from legal liabilities and to inform employees about how they may and may not use the school computer facilities.

3. Access

The school will provide access to e-mail and the Internet to all employees for work related purposes.

- A) Access to the Internet is only permitted with the recorded approval of the head teacher or their delegated representative;
- B) All access must be in a manner approved by and arranged through the head teacher or their delegated representative;
- C) Any data or information downloaded from the Internet must not be loaded to any other PC, networked or otherwise, until the data has been checked for viruses. It is the user's responsibility to ensure that this done.

4. Acceptable Use

E-Mail provides a speedy, effective means of communicating information to colleagues, school contacts, suppliers and outside agencies; however, it is capable of being used for inappropriate purposes.

You should not transmit anything in an email that you would not be comfortable writing in a letter or memo. It is important to be aware that electronic messages are admissible as evidence in legal proceedings and have been successfully used in libel cases.

You should therefore, refrain from sending vast quantities of material via e-mail or e-mail attachments. You should not assume that internal messages are necessarily private and confidential, even if marked as such. Matters of a sensitive or personal nature should not be transmitted by e-mail.

It is important that you may not at any time use mobile phones, e-mail or the Internet for any of the following purposes:

- To communicate information that is confidential to the school
- When writing e-mails, do not present any views and opinions that you may personally hold as views of the school
- To access, view or download pornography, or any other type of offensive material on the Internet
- To communicate anything by e-mail that could be interpreted as defamatory, discriminatory, derogatory or offensive, whether internally or externally
- To allow individual pupils to have their own unsupervised e-mail address at school (for child protection reasons)

Use of a personal mobile phone in school, whether during work or break times, to communicate, access, view or download pornography, or any other type of offensive material that could be interpreted as defamatory, discriminatory, derogatory or offensive, will not be tolerated.

The above activities will be regarded as gross misconduct which may, after proper investigation, lead to your dismissal. If you are at all unsure about the use of e-mail or the Internet, advice or clarification must be sought from the headteacher.

5. Personal and Private Use

It is recognised that employees may sometimes need to attend to personal matters during working hours; therefore, the school may at its discretion permit limited use of the school's telephones, e-mail and Internet access. Reasonable personal use of e-mail means use either outside of working hours or occasionally, and very briefly, during working hours provided that such use is not excessive and does not disrupt day to day work and performance of work tasks. Employees will normally be expected to confine personal e-mail use to their lunch breaks or break periods. The school will not make a charge for this provided that the privilege is not abused.

Mobile Phones

It is recognised that employees may sometimes need to attend to personal matters during working hours; therefore, the school may at its discretion permit limited use of personal mobile phones. Reasonable personal use of mobile phones means use either outside of working hours or occasionally, and very briefly, during working hours provided that such use is not excessive and does not disrupt day to day work and performance of work tasks. Employees will normally be expected to confine personal mobile phone use to their lunch breaks or break periods.

6. Security and Confidentiality

Employees are responsible for the PC that they are using and should not leave their workstation logged on and unattended.

Passwords must be confidential and should not be disclosed to anyone else unless prior written authority to do so is obtained by the head teacher or the delegated representative.

In order to avoid the risk of viruses entering the system, employees must not load unauthorised software on to the system or download software from the Internet. E-mail attachments should not be opened from an unknown sender or from any source where virus protection may not be current and active.

7. Monitoring

The school's telecommunication system is school property therefore, telephone calls made and e-mail messages sent and received and Internet sites accessed cannot be regarded as private.

The school respects the rights of individuals to privacy of communication, yet at the same time, it has a right and duty to protect the interests of staff and pupils against unlawful use of its systems. Consequently, the school reserves the right to intercept or access personal and private communications if there are reasonable grounds to show the likelihood of some crime having been committed or of unlawful or unauthorised use of the system. In such circumstances and before any action is taken, advice will be sought from Schools Service Personnel.

Any monitoring will conform with the provisions of the Telecommunications (lawful Business Practice) (Interception of Communications) Regulations 2000, the Human Rights Act 1998 and the Data Protection Act 1998.

8. Whistle blowing

If an employee is concerned that a colleague is abusing the school systems or acting in a way that is contrary to the policy, they are encouraged to disclose the abuse in confidence either to their line manager or to the Head teacher. No employee will be penalised for raising a genuine concern with management about issues they have regarding instances of e-mail or Internet abuse. If you do not feel that you can disclose information to management please contact Schools Service Personnel for advice and guidance.

Policy for Employee use of E-mail, the Internet, Personal Mobile Phones and Rochdale's Intranet

Acceptance

I have received a copy of this policy and agree to the terms and conditions contained therein.

Name _____

Signature _____

Date _____

Appendix 18 – ‘Rules for Responsible Internet Use’

Smithy Bridge Foundation Primary School

Rules for Responsible Internet Use

The school has installed computers with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.



Using the computers

- I will only access the computer system with permission from a member of staff
- I will not access other people's files
- I will not bring in floppy disks or CDs from outside school and try to use them on the school computers



Using the Internet

- I will ask permission from a teacher before using the Internet
- I cannot use the Internet without a member of staff being present
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself
- I understand that the school may check my computer files and may monitor the Internet sites I visit
- I will not complete and send forms without permission from my teacher
- I will not give my full name, my home address or telephone number when completing forms.



Using e-mail

- I will ask permission from a teacher before checking the e-mail
 - I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself
 - I understand that others may read e-mail messages I receive or send
 - The messages I send will be polite and responsible
 - I will only e-mail people I know, or my teacher has approved
 - I will only send an e-mail when a teacher has checked it
 - I will not give my full name, my home address or telephone number
 - I will not use e-mail to arrange to meet someone outside school hours
-

Please complete and return this form to the Headteacher.

Use of Internet

Pupil (Years 2,3,4,5 and 6 only)

I have read and understood the school Rules for Responsible Internet Use, and agree to comply with them. I will use the Internet, e-mail and other facilities at school in a safe and responsible way and observe all the restrictions explained to me by the school.

Pupil's signature _____ Date _____

Parent

I have read and understand the school rules for responsible Internet and email use. As the parent or legal guardian of the pupil signing above, I understand that the school will take reasonable precautions to ensure that pupils can not access inappropriate materials, including the teaching of Internet safety skills to pupils, but accept that ultimately the school can not be held responsible for the nature and content of materials accessed through the Internet. I accept responsibility for setting and conveying standards for my son or daughter to follow when selecting, sharing and exploring information and media, and acknowledge that they will be deemed to be accountable for their own actions.

Signed _____ Date: ____/____/____

Pupil's name _____

Class _____

Use of images on school web site, local and national press

Including images of pupils on our school website or in the local press can be motivating for the children involved and provide a good opportunity to promote the work of the school.
In order for us to consider the safety of your child, we need to have your permission for such images to be used.

***I give/ do not give** permission for the image of my child / children to be used in local and national press publications. The child's name may be used in the newspaper.

Signed _____

***I give/ do not give** permission for the image of my child / children to be used on the school web site. I understand that children's names will not be used.

Signed _____

*** PLEASE DELETE AS APPROPRIATE**

Appendix 19 – ‘Record for Reviewing Devices/Internet Sites

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

--

Web site(s) address / device

Reason for concern

Conclusion and Action proposed or taken

Appendix 20 – ‘Reporting Log’

Template Reporting Log

[illegible]

Appendix 21 – Advice on Safe Search Engines

Advice - Safe Search Engines

Although we endeavour to filter as much of the internet content as we can using technology to scan and assess the content of websites it can never be guaranteed as 100% effective. We choose to operate a managed filter system whereby sites and pages are categorised based on their content, rather than a restricted filter system which simply states what websites you can and can't use. The managed filter system is used highlighted as being the option of choice by schools rated as outstanding in relation to e-safety by Ofsted as it helps children to learn correct practices and make appropriate choices about internet use (*Feb 2010, The Safe Use of New Technologies, Ofsted*).

Therefore when children search the internet, our filtering *sometimes* struggles, particular as children can choose to intentionally put in words which will produce unwanted sites and images. Additionally some images and sites have innocently sounding names to a child but actually portray potentially offensive material. Although our filters are updated regularly with new data, the internet is updated with new content with equal regularity. The following sites have been looked at as a benchmark for safe searching. We would recommend schools use these or similar in order to avoid unnecessary problems. Please note that, as with all search engines, they are not 100% effective unless the content has been pre-approved, i.e. a human has checked it first.

KidRex <http://www.kidrex.org/>

KidRex is a custom Google search engine for kids. The interface is just like a child's crayon drawing (the dinosaur stands guard). It uses SafeSearch and tries to keep all the results as antiseptic as possible.

KidRex also has its own database of inappropriate websites and keywords which further help to keep the results clean.

Google Safe Images <http://www.google.safesearchkids.com/>

This safe image search tool is text based. This provides additional safety by filtering Image Titles and Descriptions using SafeSearch. This also allows for safe searching of images without worrying about individual computer settings because safe search is locked on this website, as explained on the Google SafeSearch page for regular web results.

When searching for images on this site, smaller images appear beside most of the search terms. Images and their descriptions are listed in search results individually. After selecting an image to view, click the back button to return to the search results. This Safe Search box overrides your computer settings to ensure strict filtering for all results.

Important Note

When you undertake a Google Image Search you are searching files stored on Google servers. They have harvested these images from the internet and hold thumbnail copies of them. Therefore all search results are based on Google's assessment of whether these are 'safe' or not even under Strict Safe Search mode.

Our filters will block websites that have been deemed inappropriate. However, in order to ensure that 100% of inappropriate *images* do not get passed through we would have to block Google Images. We do not believe that school's would appreciate this and therefore we rely on Google's assessment of Strict Safe Search. This is not 100% reliable and therefore we would recommend staff follow these simple rules:

- ☑ Always use two or more words as search parameters
- ☑ Always check your search parameters at most 1 hour before you wish to undertake this with pupils to make you aware of any possible issues, i.e. do a dummy run yourself including making some spelling mistakes or missing/adding plurals
- ☑ Always monitor pupil's use of the internet when undertaking "free" searches

If inappropriate thumbnail images are generated from a Google image search the underlying link to the website should not work.

Appendix 22 – ‘5 Smart Rules for Staying Safe’



stay safe online

Remember the 5 SMART rules when using the internet and mobile phones.

- S SAFE** Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
- M MEET** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
- A ACCEPTING** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
- R RELIABLE** Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.
- T TELL** Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Find out more at Childnet's website ...

www.kidsmart.org.uk

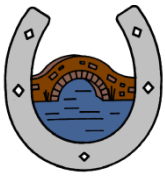
Childnet International © 2002-2007 Registered Charity no. 1080173 www.childnet.com

Childnet International Kid Smart

Appendix 23 – Internet Safety poster



Appendix 24 – Smithy Bridge ‘Hints & Tips for Parents’



Smithy Bridge E-Safety Advice for Parents & Carers

Hints and Tips

- Technology is constantly changing and young people are continually learning - keep up to date with the latest developments so you know about the risks
 - Online safety applies to all types of devices - PCs, laptops, tablets, smartphones, e-readers and online gaming
 - As technology becomes more portable, set guidelines for where your child could/should use their device
 - Treat online safety in the same way as you would offline safety such as stranger danger, crossing the road etc..
 - Set up internet security so children can't access websites with inappropriate content
 - Don't write anything online that you wouldn't say in person. Comments made on social media and/or public web pages/forums could reflect badly on your child
 - Cyber bullying should be treated in the same way as other forms of bullying; contact school to agree a plan to deal with it
 - Try to establish a system which allows your child to talk to you about anything they feel uncomfortable about online
-

Things to Discuss with Children

- Where is it acceptable to use your portable device?
 - Who should you talk to if you feel uncomfortable about something you have seen online? E.g. parent, teacher or other responsible adult
 - Don't spend too long online; make sure you get some physical exercise each day
 - Keep passwords safe - don't write them down and change them regularly
 - What personal information is appropriate to post online?
 - How do you report cyber bullying? Take a screen grab/photo of any posts so they can be seen at a later date if needed
 - How do you know the people you are talking to online are who you think they are?
 - What is the difference between a 'real life' friend and an 'online' friend?
 - Is it sensible to meet up with an 'online' friend?
 - Who are you in contact with when you play games online?
 - Do you know you have to be 13 to have a Facebook account?
-

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see [template policy in these appendices and for DfE guidance - <http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>](#))

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations>

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

[Safer Internet Centre -](#)

[South West Grid for Learning](#)

[Childnet](#)

[Professionals Online Safety Helpline](#)

[Internet Watch Foundation](#)

CEOP

<http://ceop.police.uk/>

[ThinkUKnow](#)

Others:

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz <http://www.netsmartz.org/index.aspx>

Support for Schools

Specialist help and support [SWGfL BOOST](#)

Cyberbullying

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government [Better relationships, better learning, better behaviour](#)

[DCSF - Cyberbullying guidance](#)

[DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies](#)

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

Social Networking

Digizen – [Social Networking](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Alberta, Canada - [digital citizenship policy development guide.pdf](#)

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Somerset - [e-Sense materials for schools](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[ICO pages for young people](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO – Access Aware Toolkit](#)

[ICO Subject Access Code of Practice](#)

[ICO – Guidance on Data Security Breach Management](#)

SWGfL - [Guidance for Schools on Cloud Hosted Services](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

Professional Standards / Staff Training

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

Kent - [Safer Practice with Technology](#)

Childnet / TDA - [Social Networking - a guide for trainee teachers & NQTs](#)

Childnet / TDA - [Teachers and Technology - a checklist for trainee teachers & NQTs](#)

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - [Questions for Technical Support](#)

NEN - [Guidance Note - esecurity](#)

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

[SWGfL BOOST Presentations - parents presentation](#)

[Connect Safely - a Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[DirectGov - Internet Safety for parents](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development

CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
