Rushton C of E Primary School

e-Safety Policy

School Policy

e-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The schools e-Safety policy will operate in conjunction with other policies including those for ICT, student behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security.

1 Writing and reviewing the e-Safety Policy (Appendix 1 – Legislation)

The e-Safety Policy relates to other policies including those for ICT, bullying and child protection.

- The schools e-Safety committee includes the Headteacher, e-Safety (ICT) Coordinator, e-Safety Governor along with a parent and a child representative from yr 3/4. At Rushton School the Headteacher also acts as the e-safety (ICT) Coordinator.
- It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was reviewed by:- _____
- It was approved by the Governors on:- _____

2 Teaching and Learning

2.1 Why internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access (Including the Learning Platform (LP)) as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Access to experts in many fields for pupils and staff.
- Access to world wide educational resources including museums and art galleries.

2.2 Internet use will enhance learning (Appendix 2 – Curriculum)

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Internet access will be planned to enrich and extend learning activities.

2.3 Pupils will be taught how to evaluate internet content (Appendix 3 – Education)

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If staff or pupils discover unsuitable sites, the URL and content must be reported to the internet service provider via the ICT Coordinator.

3 Managing Internet Access (Appendix 4 – Unsuitable Activities, 5 – Password Security, 6 – Technical)

3.1 Information systems security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- All curriculum machines have Forensic monitoring software installed.

3.2 e-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group email address should be used at Key stage 2 and below.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

3.3 Published content and the school web-site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupils images and work (Appendix 7 – Use of digital & video images – photographic, video)

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site, via the Digital/Video images permission form.

3.5 Social networking and personal publishing

- The school/LEA will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

3.6 Managing filtering (Appendix 8 – Filtering)

- The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing video conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

3.9 Protecting personal data (Appendix 9 – Data Protection, 10 – Data Handling)

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Rushton C of E Primary School

4 Policy Decisions

4.1 Authorizing internet access (Appendix 11 – Acceptable use policy)

- All staff & pupils must read and sign their respective Acceptable Use Agreement before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access may be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

4.2 Accessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Staffs LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

4.3 Handling e-Safety complaints (Appendix 12 – Incidents of misuse)

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

4.4 Community use of the internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Rushton C of E Primary School

5 Communications policy (Appendix 13 – Communications, 14 Logon Statement)

5.1 Introducing the e-safety policy to pupils

- E-safety rules (AUP) will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

5.2 Staff, Governors, Pupils, Parents/Carers, Community Users and the e-safety policy (Appendix 15 – Roles)

- All parties will be given/have access to the School e-Safety Policy so as to review its importance.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

5.3 Enlisting parents support

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school Web site.

Rushton C of E Primary School

Appendix 1

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.

Rushton C of E Primary School

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.

Rushton C of E Primary School

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 who 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.

Rushton C of E Primary School

Appendix 2

e-Safety Curriculum

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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, e.g. using search engines, staff should 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 (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Coordinator can temporarily remove those sites from the filtered list for the period of study (may also require approval from SLT). Any request to do so, should be auditable, with clear reasons for the need. Requests for website release should be made on an appropriate request pro-forma.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism, particularly with respect to examination coursework..

Rushton C of E Primary School

Appendix 3

e-Safety Education

Pupils

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 education will be provided in the following ways:

- **A planned e-Safety programme should be provided as part of ICT / PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies (LP) in school and outside school.**
- **Key e-Safety messages should be reinforced as part of a planned programme of assemblies / pastoral activities.**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide".

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

- *Letters, newsletters, web site, Learning Platform, DVD.*
- *Cluster Parents evenings.*

Rushton C of E Primary School

Education & Training – Staff

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:

- **e-Safety training will be made available to staff.**
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**
- *The e-Safety Coordinator (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by *****BECTA / LA and others.*
- *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 (or other nominated person) will provide guidance as required to individuals as required*

Training – Governors

Governors should take part in e-Safety awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / 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 information sessions for staff or parents

* The school is aware of the Government's decision to close BECTA see

http://www.education.gov.uk/aboutdfe/armslengthbodies/a00192537/becta

Rushton C of E Primary School

Appendix 4

e-safety Unsuitable / inappropriate / illegal activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and those 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 certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					√
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					√
	adult material that potentially breaches the Obscene Publications Act in the UK					√
	criminally racist material in UK					√
	pornography				√	
	promotion of any kind of discrimination				√	
	promotion of racial or religious hatred				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	
	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				√	
Using school systems to run a private business					√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					√	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					√	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	

Rushton C of E Primary School

Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				√	
On-line gaming (educational)				√	
On-line gaming (non educational)				√	
On-line gambling				√	
On-line shopping / commerce			√		
File sharing			√		
Use of social networking sites				√	
Use of video broadcasting e.g. Youtube			√		

Rushton C of E Primary School

Appendix 5

Password Security Policy

Introduction

The school will be responsible for ensuring that the school infrastructure / network / Learning Platform is as safe and secure as is reasonably possible and that:

- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email.

Responsibilities

The management of the password security policy will be the responsibility of the ICT Coordinator.

All users (adults and young people) will have responsibility for the security of their username and password.

Training / Awareness

It is essential that all users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and / or e-safety lessons (PHSE)
- through the Acceptable Use Agreement

Visitors / Contractors / Members of the wider community will be made aware of the school's password policy

- Through the Acceptable Use Agreement

Rushton C of E Primary School

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Coordinator and will be reviewed, at least annually, by the e-Safety Committee.

Audit / Monitoring / Reporting / Review

The ICT Coordinator will ensure that full records are kept of:

- User Id's and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification (IL4) and stored in a secure manner.

These records will be reviewed by the *E-Safety Committee* at regular intervals *(Termly).*

This policy will be regularly reviewed (preferably annually) in response to changes in guidance and evidence gained from the Forensic logs.

Rushton C of E Primary School

Appendix 6

Technical – infrastructure / equipment, filtering and monitoring

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 appropriate sections will be effective in carrying out their e-safety responsibilities:

- **School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority e-Safety Policy and guidance**
- **There will be regular reviews and audits of the safety and security of school ICT systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**

- **All users will have clearly defined access rights to school ICT systems.** Details of the access rights available to groups of users will be recorded by the ICT Coordinator and will be reviewed, at least annually, by the e-Safety Committee.
- **All users have access via a generic password to any computer in the classroom.**
- The school maintains and supports the managed filtering service provided by the LA
- The school has provided enhanced user-level filtering through the use of the Forensic filtering programme.
- Any filtering issues should be reported immediately to SLT (Staffordshire Learning Technologies).
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Coordinator. If the request is agreed by SLT, this action will be recorded and logs of such actions shall be reviewed by the e-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- An appropriate system is in place for users to report any actual / potential e-safety incident to the ICT Coordinator and e-Safety committee.
- Guests (e.g. trainee teachers, visitors) who wish to log onto the school system will abide by the schools e-Safety policy.
- An agreed policy is in place whereby the ICT Coordinator will either allow staff to / forbid staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices. (See Rushton School Personal Data Policy, App 10)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See Rushton School Personal Data Policy, App 10)

Rushton C of E Primary School

Appendix 7

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 e.g. on social networking sites.**
- Staff 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 must **not** be used for such purposes.
- Care should be taken when taking digital / video images that 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 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, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Parents/carers may withdraw consent at any time by making a written notice to the school.
- We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Please note

The press, in certain circumstances are exempt from the Data Protection Act and may want to include the names and personal details of children and adults in the media.

Parents, family members and friends taking photographs of children within school at events such as plays and sports day for their personal, domestic use is also exempt from the Data Protection Act and therefore do not need to gain consent.

Rushton C of E Primary School

IL4 – Confidential

Use of Digital / Video Images Agreement

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their surnames.
Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name

Pupils Name

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed

Date

Rushton C of E Primary School

Appendix 8

Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the Staffordshire Learning Network schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT Coordinator. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:-

- **be reported to a second responsible person (Headteacher):**
- be reported to and authorised by a second responsible person prior to changes being made (Chair of Governors).
- be reported to the E-Safety Governor every month.

All users have a responsibility to report immediately to (ICT Coordinator) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through newsletters.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (ICT Coordinator) who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at county level, the responsible person (ICT Coordinator) should contact Staffordshire Learning Technologies with the URL.

Rushton C of E Primary School

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School e-Safety Policy and the Acceptable Use agreement. Rushton School uses Forensic Monitoring.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Headteacher)
- E-Safety Committee
- E-Safety Governor / Governors committee
- Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Rushton C of E Primary School

Appendix 9

e-Safety Data Protection Policy

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.

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, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Rushton does not use Biometrics in school.

Rushton C of E Primary School

Appendix 10

School Personal Data Handling Policy

Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (BECTA – Good Practice in information handling in schools – keeping data secure, safe and legal – March 2009). For information on how this is managed now that BECTA has been disestablished see:- http://www.education.gov.uk/aboutdfe/armslengthbodies/a00192537/becta

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it can not be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “LA Privacy Notice” http://education.staffordshire.gov.uk/SchoolAdministration/PupilDatabase/Fair+Processing/ and lawfully processed in accordance with the “Conditions for Processing”.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references and SEN.
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members (including attendance records).

Rushton C of E Primary School

Responsibilities

The school's Senior Information Risk Officer (SIRO) is the Headteacher. The Headteacher will keep up to date with current legislation and guidance and will:-

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owner (IAO)

The schools Information Asset Owner (IAO) is the Office Support Manager who will be responsible for all types of data being held (e.g. pupil / student information / staff information / assessment data etc). The IAO will manage and address risks to the information and will understand:-

- what information is held and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

Rushton School adopts the guidance given by *BECTA in their "Good Practice in information handling in schools" document, that is applicable for a school of Rushton's size.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Display equipment must be positioned so that the screen display is not visible to any unauthorised persons.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Notification (Data Protection Register) held by the Information Commission Officer (ICO) based in Wilmslow.

Information to Parents / Carers – the "LA Privacy Notice"

Under privacy requirements in the Data Protection Act, the school will inform parents / carers of all pupils / students of the data they hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DCSF, QCA, etc) to whom it may be passed. This "Privacy Notice" will be passed to parents / carers through the school website and specific letters. Parents / carers of young people who are new to the school will be provided with the privacy notice through a specific letter (see end of section for current notice).

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:-

- Induction training for new staff
- Staff meetings / Inset
- Day to day support and guidance from Information Asset Owner and newsletters such as the "Data Protection & Freedom of Information" issued by the LA.

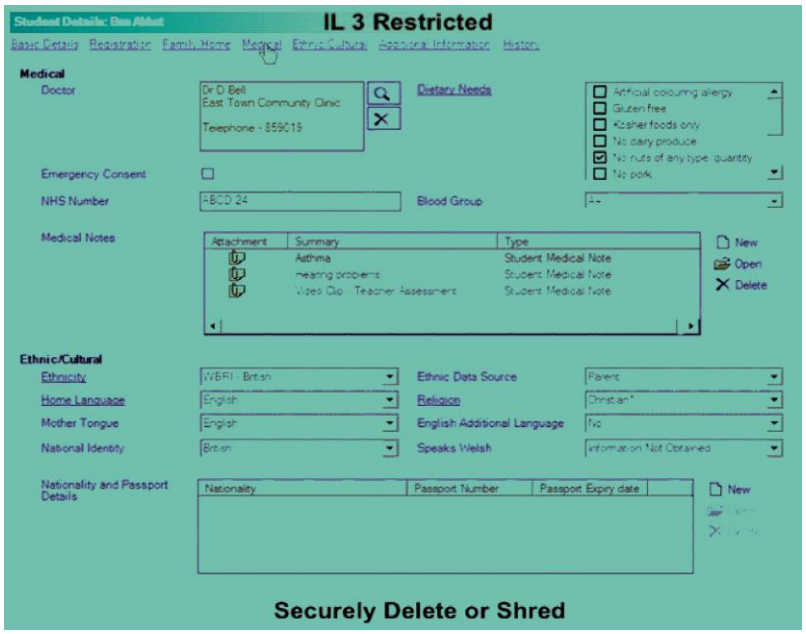
Identification of data

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer:

* The school is aware of the recent Government decision to close BECTA see http://www.education.gov.uk/aboutdfe/armslengthbodies/a00192537/becta

Rushton C of E Primary School



Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect
- IL3–Restricted
- IL4–Confidential

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data.

Release and destruction markings will be shown in the footer as follows

[Release]	[Parties]	[Restrictions]	[Encrypt, Securely delete or shred]
The authority descriptor	The individuals or organisations the information may be released to	Descriptor tailored to the specific individual	How the document should be destroyed
Examples:			
Senior Information Risk Owner	School use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information to father ASBO	Securely delete or shred

Rushton C of E Primary School

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users with access to sensitive data will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media, where allowed). Private equipment (i.e. owned by the users) must not be used.

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot 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 once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (Subject Access will be referred to the ICO Wilmslow) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Rushton C of E Primary School

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log is kept in the school office of all data that is disposed of. The log includes the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

Due to the nature and size of Rushton School, any incidents will be investigated by the SIRO with assistance from the IAO. If necessary this will be reported to the ICO for support and record keeping.

Rushton C of E Primary School

Privacy Notice 2015-2016

Privacy Notice - Data Protection Act 1998

PRIVACY NOTICE
for

Pupils in Schools, Alternative Provision and Pupil Referral Units and Children in Early Years Settings

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

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

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE). Where appropriate we will send to relevant National Health Service personnel (e.g. school nurses, the NHS Health Informatics Team) information on individual pupils changing school (or address) to ensure continuity of health care.

If you want to see a copy of the information about you that we hold and/or share, please contact **the school office (Rhiannon Capewell)**
If you require more information about how the school, Local Authority (LA), Entrust and/or DfE store and use your information, then please go to the following websites:

www.rushton.staffs.sch

http://www.staffordshire.gov.uk/health/childrenandfamilycare/yourdata/Yourdata.aspx

Rushton C of E Primary School

and

http://www.education.gov.uk/researchandstatistics/datatdatam/privacynotices/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- Information Governance Unit
  Staffordshire County Council
  St Chad's Place
  Stafford
  ST16 2LR
  e-mail: foi@staffordshire.gov.uk

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  Website: www.education.gov.uk
  email: http://www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288

Rushton C of E Primary School

Appendix 11

Pupil Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT and Learning Platform to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line, unless under the supervision of the teaching staff.
- I will never arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Rushton C of E Primary School

IL4 - Confidential

Rushton Pupil Acceptable Use Agreement

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have had Rushton School's Pupil Acceptable Use Policy explained to me and agree to follow these guidelines when:

- I use the school ICT systems, Learning Platform and equipment (both in and out of school)
- I use my own equipment, out of school, in a responsible way.

Also I will **not** use my own equipment in school e.g. mobile phones, PDA's, cameras and other games devices etc, unless I have been given permission to do so by the teaching staff.

Name of Pupil			
Group / Class			
Signed		Date	

Rushton C of E Primary School

Staff (and Volunteer) Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDA's / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems, unless it relates to school business.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed by the ICT Coordinator.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Personal Data Handling Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Rushton C of E Primary School

IL4 - Confidential

Rushton Staff (and volunteer) Acceptable Use Agreement

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Rushton C of E Primary School

IL4 – Confidential

Parent / Carer Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Pupils Name	

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed		Date	

Rushton C of E Primary School

Appendix 12

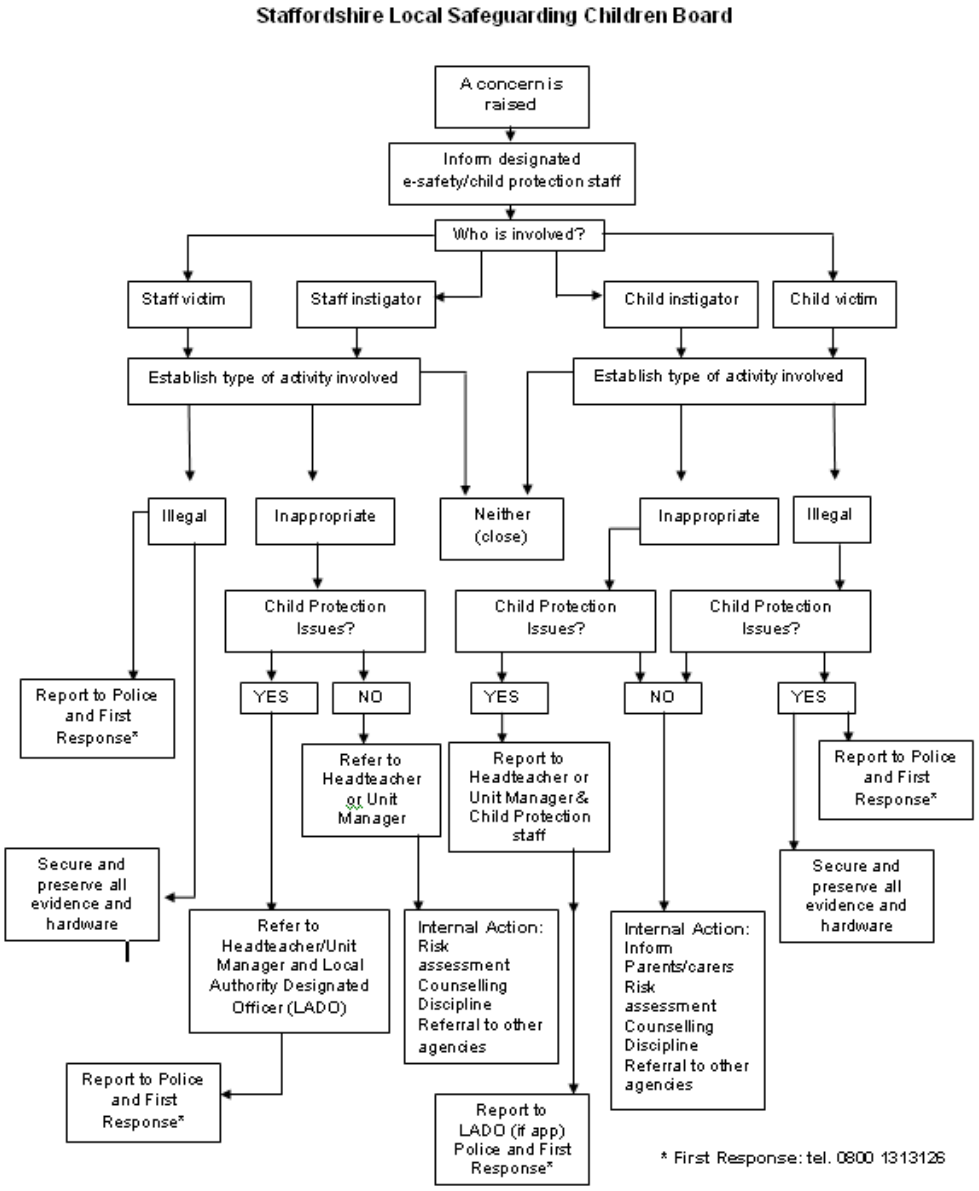
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The flow chart from the Staffordshire Safeguarding Children's board– below and http://www.staffsscb.org.uk/professionals/esafety/e-SafetyToolkit/IncidentResponse/ should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event contact will be made with the Staffordshire Safeguarding Children's Board

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 (the tables that follow are a guide and are not statutory as each individual case differs):-

Rushton C of E Primary School

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to ICT Coordinator	Refer to Headteacher \ e-Safety committee	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 e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			√	√		√			
Unauthorised use of non-educational sites during lessons	√								
Unauthorised use of mobile phone / digital camera / other handheld device	√	√				√			
Unauthorised use of social networking / instant messaging / personal email	√	√	√			√			
Unauthorised downloading or uploading of files		√							
Allowing others to access school network by sharing username and passwords		√							
Corrupting or destroying the data of other users	√	√							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√			√			
Continued infringements of the above, following previous warnings or sanctions			√						√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√	√			√		√	√
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√							
Deliberately accessing or trying to access offensive or pornographic material	√	√	√			√			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		√	√						

Rushton C of E Primary School

Staff Actions / Sanctions

Incidents:	Refer to le-Safety committee	Refer to Headteacher	Refer to Local Authority / HR	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).	√	√	√	√		√	√	√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√	√				√		
Unauthorised downloading or uploading of files	√							
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	√	√				√		
Careless use of personal data e.g. holding or transferring data in an insecure manner	√							
Deliberate actions to breach data protection or network security rules		√				√		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√	√					√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√				√		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	√	√				√		
Actions which could compromise the staff member's professional standing		√				√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√				√		√
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√						
Deliberately accessing or trying to access offensive or pornographic material	√	√				√		
Breaching copyright or licensing regulations	√	√						
Continued infringements of the above, following previous warnings or sanctions		√				√		√

Rushton C of E Primary School

Appendix 13

e-Safety Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√						√	
Taking photos on personal mobile phones or other camera devices				√				√
Use of hand held devices e.g. PDAs, PSPs	√						√	
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails				√				√
Use of chat rooms / facilities				√				√
Use of instant messaging		√						√
Use of social networking sites				√				√
Use of blogs				√				√

Rushton C of E Primary School

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored.** Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- **Users need to be aware that email communications may be monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and pupils or parents / carers (email) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- whole class or group email addresses will be used at KS1 & KS2
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Rushton C of E Primary School

Appendix 14

Generic Logon AUP Statement

This room has Internet access to help users learn.

Posted on the wall of this room are a set of rules that you need to read and agree to.

These rules will keep everyone safe and help us be respectful of other users

Wall copy of specific rules

Rushton School classrooms/resource rooms have Internet access to help users learn.

These rules will keep everyone safe and help us be respectful of other users

- I will only access the system with the login and password provided
- I will not access other people's files
- I will only use the computers for work related activities
- I will not use CD's or other computer media unless I have been given permission
- I will ask permission from a member of staff before using the Internet
- I will only e-mail people I know for work/learning related purposes
- The messages I send will be polite and responsible
- I will not give out personal information
- I will report any unpleasant material or messages I find or sent to me
- I understand that there will be checks and monitoring of computer use and the Internet sites I visit
- I understand reports will be confidential and will help protect myself and others

Rushton C of E Primary School

Appendix 15

e-Safety Roles and Responsibilities

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

Governors:

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 e-Safety Governors Committee 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 .The role of the e-Safety Governor will include:

- regular meetings with the e-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- **The Headteacher is responsible 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 / Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the e-Safety Co-ordinator.
- **The Headteacher and 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 SSCB website or APPENDIX 1of the e-Safety policy for a flow chart on dealing with e-safety incidents).

Rushton C of E Primary School

e-Safety Coordinator:

- leads 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
- 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
- any sanctions necessary will be applied by the Headteacher

Network Manager (ICT Co-ordinator)

ICT Co-ordinator is responsible for ensuring:

- **that the school's ICT infrastructure is secure and is not open to misuse or malicious attack (managed by Staffs LEA).**
- **that the school meets the e-safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority e-Safety Policy and guidance**
- **that users may only access the school's networks through a properly enforced password protection policy.**
- Staffordshire Learning Network provides schools with the RM solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied. Schools are able to control their own permissions and add/amend to the defaults. Staffordshire Learning Technologies can be contacted if schools require assistance with this.
- that he / she keeps 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.
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Co-ordinator for investigation / action.
- that monitoring software / systems are implemented and updated.

Rushton C of E Primary School

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 school Staff Acceptable Use Policy (AUP).**
- **they report any suspected misuse or problem to the e-Safety Co-ordinator /Headteacher for investigation / action / sanction.**
- **digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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

Designated person for child protection / Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child protection 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

Rushton C of E Primary School

e-Safety Committee

Members of the e-Safety committee will assist the e-Safety Coordinator with:

- the review / monitoring of the school e-Safety policy / documents.
  The e-Safety committee comprises the e-Safety Co-ordinator, e-Safety Governor, Headtecher, a Parent, a year 3 or 4 child.

Pupils:

- **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.**
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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.**

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through, newsletters, letters, website, literature. Parents and carers will be responsible for:

- **endorsing (by signature) the Pupil Acceptable Use Policy**

Community Users

There are no current users, but should this change the policy will be reviewed.