The Bath & Mendip Partnership Trust

ONLINE SAFETY POLICY

THE MENDIP SCHOOL

POLICY DATE

WRITTEN BY **JAKE GODFREY**

DATE WRITTEN **12TH OCTOBER 2018**

REVIEWED: **SEPTEMBER 2019**

POLICY REVIEWS

LENGTH OF POLICY **3 YEARS**

REVIEW DATE **12TH OCTOBER 2022**

REVIEW BY **ICT SUBJECT LEADER AND NETWORK MANAGER**

APPROVED BY GOVERNORS

DATE APPROVED **OCTOBER 2018**

Online safety Policy

Safeguarding Children and Protecting Staff

Reviewed 26.09.19

Contents

Background / Rationale

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

There may be times when professional judgements are made in situations not covered by this document, or directly contravene the standards outlined in this document. It is expected that in these circumstances that staff will advise a member of SLT of any such action. The SLT will in turn seek advice and log any activity.

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 'Guidance for safer working practice for adults who work with children and young people' policy and 'Keeping Children Safe in Education, September 2019'. A school online safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher of the school and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful, unsuitable or inappropriate content.
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying, Online peer to peer bullying or 'Trolling'
- Identity fraud
- Access to poor quality, inaccurate and irrelevant information
- Plagiarism and copyright infringement
- Illegal file sharing
- Excessive use which may impact on the social and emotional development and learning of the young person
- Sexting
- Serious Violence
- Upskirting

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies:

- Behaviour Policy
- Guidance for Safer Working Practice for Adults who work with Children and Young People
- Keeping Children Safe in Education 2019
- Child Protection Policy
- Disciplinary Policy and Procedures
- Equal Opportunities Policy
- Code of Conduct Policy
- Health and Safety Policy
- Acceptable Use of ICT Policy

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The Mendip School will demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors and community users) who are users of school ICT systems including use on personal devices.

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

This is pertinent to online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
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 online behaviour that take place out of school.

This policy is designed to cover all technologies that are used within the School Community both on and off site.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Senior Leadership

- The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead
- The Senior Leadership Team are responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Senior Leadership Team Leaders will ensure that there is a system in place to support and regulate those in school who carry out the internal online safety monitoring role.
- The Senior Leadership Team will receive monitoring reports from the Designated Safeguarding Lead when appropriate.
- The Head teacher and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with online safety incidents and relevant policies)

Network Manager / Technical staff

The Network Manager is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the online safety technical requirements outlined in the relevant policies
- That users may only access the school's networks through a properly enforced password protection policy.
- SWGfL is informed of issues relating to the filtering applied by the Grid
- The school filtering policy is applied and reviewed on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy")
- That he / she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the computing Co-ordinator or ICT helpdesk for investigation, action or sanction

- That monitoring software / systems are implemented and updated as agreed in school policies

Members of the School Community

Are responsible for ensuring that:

- Their actions, behaviour and conduct should avoid any reasonable person to question their motivation and intentions.
- They work and should be seen to work in an open and transparent way.
- They continually monitor and review their practice in terms of the evolving world of learning technologies
- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy
- They report any suspected misuse or problem to their Line Manager for investigation, action or sanction
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school online safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, tablets, 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 students 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 Safeguarding Lead

Should be trained in online 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 online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting
- Upskirting

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

The DSL should also:

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with Network Manager to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

Policy Statements

Education – Students

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

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of ICT and PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students 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 displayed in learning areas
- Where students are allowed to freely search the internet, eg 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list as identified in the Technical Policy Statement.
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online 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 online 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". (Byron Report).

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

- Letters, newsletters, web site, school's social media
- Parents evenings
- Reference to the "Know-IT-all" website
- Parent forums

Education - Community

The school will offer learning support in ICT, media literacy and online safety so that the community can together gain a better understanding of these issues. Messages to the public around online safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

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

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety guidance as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online safety Coordinator (or other nominated person) will receive regular CPD on Online safety
- This Online safety policy and its updates will be reviewed and disseminated when appropriate
- The Online safety Coordinator will provide support as required

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 above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy, GDPR and Acceptable Usage Policy and any relevant Local Authority Online 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 Network Manager and will be reviewed annually
- All users will be provided with a username and password where appropriate by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password regularly. The Mendip school will ensure each child has an individual log in and password
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacheror other nominated senior leader and kept in the school safe in the Black files room.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Any filtering issues should be reported immediately to Network Manager/ICT co-ordinator
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager/ICT co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online safety Committee
- Student User activity is only looked at when requested by staff or when faults on the network are traced to them.
- Staff User activity is NOT generally observed and personal data and email will never be, unless authorised in writing by the Head teacher.
- Remote management tools are used by staff to control workstations and view users activity
- Users must report any actual / potential online safety incident to the Network Manager or ICT coordinator.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental

or malicious attempts which might threaten the security of the school systems and data.

- Guests are given access to the school network with the same rights as a student. The wireless password is changed regularly.
- The Mendip School operates a policy of restricting the ability of all users to download, save and run executable files from the internet or removable media
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school. (See School Personal Data Policy Template in the appendix for further detail)
- The Mendip School forbids staff from installing programmes on school workstations / portable devices, except in the case of Teacher iPads, where educational apps can be installed for investigation and teaching purposes.
- The Mendip school allows the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in conjunction with the School Personal Data Policy (see this in the appendix for further detail)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy for further detail)

Use of Digital Media - Photographic, Video and Audio

Staff and students need to be aware of the risks associated with sharing digital media. This media may remain available accessible and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the potential for harm:

- When using digital images, staff should inform and educate students 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 record digital media to support educational aims, but must follow school policies concerning the sharing, distribution and publication of the media.
- Staff must inform the ICT Co-ordinator of use of personal devices to record media.
- Digital Media can be recorded on personal devices (in exceptional circumstances). This media must be transferred to the school network at the first opportunity and must be deleted before the end of the working day. It is highly discouraged by SWGfL but can be done so with the Head Teacher's permission.
- Care should be taken when recording digital media that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Learners must not take, use, share, publish or distribute images of others without appropriate permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' 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 digital media recordings of students are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix)

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the GDPR Act 2018 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 data, minimising the risk of its loss or misuse.
- Use data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” or “locked” when leaving the device.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any device or external media:

- The device must be encrypted or password protected.
- The device must not compromise the security of the school system. If in doubt it is the responsibility of the individual to liaise with the network manager to ensure compliance
- The data must be securely deleted from the device once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school manages the risks of new and innovative technologies.

	Staff & other adults				Students			
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	X				x			
Use of mobile phones in lessons		x					X	
Use of mobile phones in social time	X					x		
Use of smart phones in a professional capacity	x				Not Applicable			
Taking photos on mobile phones or other camera devices		X						x
Use of hand held devices e.g. PDAs, PSPs	X					X		
Use of personal email addresses in school, or on school network		X					X	
Use of school email for personal emails		X					X	
Use of chat rooms / facilities		X					X	
Use of instant messaging	x						X	
Use of social networking sites		X					X	
Use of blogs		X					X	
Use of Games Console in school time		X					X	

The above applies to all learners deemed appropriate by class teachers. See appendix

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

- Adults within the school should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which could be misinterpreted. They should report any incident with this potential to the ICT Co-ordinator, who will record as appropriate
- In their own interests, adults within school settings need to be aware of the dangers of sharing personal information. Information that could identify your profession or the school where you work should be protected
- All adults, particularly those new to the school, should review any personal information in the public domain to ensure that the information is accurate and appropriate. All accounts should be locked into the highest privacy settings and reviewed regularly. This includes any photographs that may cause embarrassment to themselves and the school
- Adults need to ensure that when they are communicating about others, even outside of school, that they give due regard to the potential for defamation of character and comply with requirements of equalities legislation
- Adults must never post derogatory remarks or offensive comments online or engage in online activities which may bring the school into disrepute or reflect negatively on their professionalism
- The official school email service may be regarded as safe and secure. Staff and students 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 electronic communication 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 students or parents / carers (email, chat, Dojo, social networks etc) must be professional in tone and content. These communications may only take place on systems developed for professional purposes and applications. Personal email addresses, text messaging, mobile phones or public chat / social networking programmes must not be used for these communications.
- Students will be provided with individual school email addresses for educational use
- Students 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.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts should be openly acknowledged and recorded by the ICT Co-

ordinator/Headteacher where there may be implications for the adult and their position within the school

- Adults should never make a “friend” of a learner at the school where they are working on social networking sites. Adults should refrain from accepting requests from ex-students where a link with the school community is maintained.

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 certain internet usage as follows:

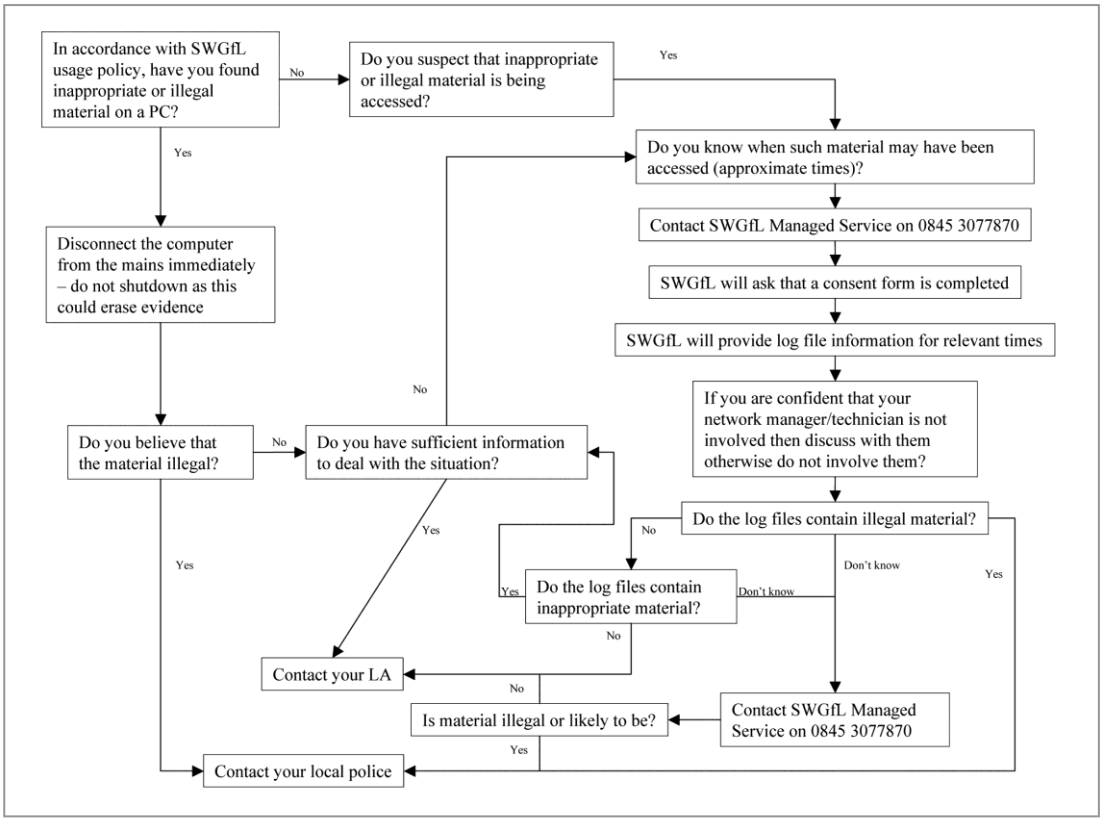
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				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	
Use systems, applications, websites or other mechanisms that bypass the monitoring or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions (On occasion ICT staff MUST carry out such procedures. Downloading software and updates. Uploading data to Backups etc.						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	
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					X	
Online gaming (educational)		X				
Online gaming (non educational)			X			
Online gambling					X	
Online shopping / commerce				X		
File sharing however, ICT staff regularly have to share files for staff/student access. They also often have to share files with external sources for fault diagnosis and other essential functions					X	
Use of social networking sites			X			

Use of video broadcasting eg Youtube		X			

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 misadventure, careless or irresponsible use or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse for most members of the school community. When dealing with incidents the ICT Coordinator will liaise with people involved and identify if the response is appropriate and proportionate. Furthermore, pupils in the SLD list will face alternative sanctions/expectations.

If any apparent or actual misuse appears to involve illegal activity, as previously identified, the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp 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 the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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 school behaviour policy or Disciplinary Policies and Procedures.

Student Actions & Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	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	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X			X	X	X	X	X
Unauthorised use of mobile phone / digital camera / other handheld device	X	X	X			X	X	X	X
Unauthorised use of social networking / instant messaging / personal email	X	X	X			X	X	X	X
Unauthorised downloading or uploading of files	X	X	X		X	X		X	X
Allowing others to access school network by sharing username and passwords	X	X	x		X	X	X	X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X		X	X	X		X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X			X
Corrupting or destroying the data of other users	X	X	X		X	X		X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X		X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	x		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Staff Actions & Sanctions

Incidents:	Refer to line manager	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).	X	X	X	X	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X	X		X	X	X	X
Unauthorised downloading or uploading of files	X	X			X	X	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 (ICT staff have occasion to carry out these type of tasks on a relatively regular basis)	X	X	X		X	X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection or network security rules	X	X	X		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X		X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X	X	X			X	X
Actions which could compromise the staff member's professional standing	X	X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X		X	X
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions	X		X	X			X	X

Acceptable Use Policies

Learner Acceptable Use of Internet and ICT 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 communication 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 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 students will have good access to ICT to enhance their learning and will, in return, expect the students 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 treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of unfamiliar contacts when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

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 online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg 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, video or audio recordings 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/laptops, tablets) 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 personal chat and social networking sites in school
- I will never invite staff to join my profile.

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.

Staff Acceptable Use of Internet and ICT Policy

(Reviewed Nov 2016)

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, efficient 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 students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff Acceptable Use of Internet & ICT 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 students 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 online 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 the professional use of any School or Personal ICT Devices
- 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 I become aware of, to the Headteacher

I will be professional in my communications and actions when using school computing 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 media.
- I will not use my personal equipment to record images or video, unless an agreement has previously been made with the ICT Co-ordinator or Network Manager. If this is the case I will make sure the media is deleted before the device is removed from the school site
- Where data is published it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policy.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online 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 (PDAs / 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 take any confidential data offsite using an external device, or personal cloud based storage, unless the data or device has been encrypted by the network manager.
- I will not use personal email addresses for school communications
- 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, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- 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 Data Protection 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 student 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.
- I will ensure when logged in to the cloud services provided by the school that I treat the PC accessing these resources the same as I would in school (locking the PC when leaving it etc.)

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)

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 normal disciplinary procedures 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 and my own devices within these guidelines.

Staff / Volunteer Name .....

Signed .....

Date .....

ICT Equipment Loan Agreement

(Reviewed Oct 2016)

Where necessary the School will provide equipment to Staff to assist in the delivery of the School curriculum. This equipment is loaned to Staff members. Whilst the equipment is in your care the following items should be noted.

- Equipment should only be used as is set out in the 'ICT Acceptable Use Policy'.
- Loaned equipment remains the property of the School and is only for use of the member of Staff that it is issued to. It is however, that member of staff's responsibility to look after the equipment whilst it is in their possession.
- Insurance cover is not provided. You are responsible for replacement if equipment is stolen whilst in your personal possession through your insurance policy (please check the details of these). Many insurance policies do not cover theft from an unattended car or accidental damage.
- Under no circumstance should Staff attempt to fix suspected hardware faults with the equipment. This must be assessed by the Network Manager before repair.
- Equipment must be returned on the termination of your employment.
- Equipment must be returned to the Network Manager/ School when requested. Appropriate notice will be given.
- Equipment damaged may not be immediately replaced. If the cost of repair is greater than the value of the equipment it will not be repaired.
- Training in the appropriate use of the equipment will be offered as part of the induction program when necessary. Refresher sessions will take place when required.
- Any charge incurred by Staff using school equipment is not chargeable back to the school.
- Failure to comply with any or all of the above may result in action in line with the disciplinary being taken and the withdrawal of the equipment.

I have read the above conditions and agree to abide by them. I am aware of the implications of insurance and recognise my responsibilities in the event of loss or damage.

Item type .....

Item Serial Number .....

Item Asset Tag .....

Staff Name .....

Signed .....

Date .....

Parent/Carer Acceptable Use of Internet and ICT 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 online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to be responsible users. 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. However, the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Pupil's activity on the ICT systems will be monitored and that the school will contact parents/carers if they have concerns.

Parents/careers should encourage the safe use of the internet and digital technologies at home and will inform the school if they have concerns over their child's online safety.

Attached is a copy of the Pupil Acceptable Use of Internet & ICT Policy so that parents / carers will be aware of the school expectations of the young people in their care.

All learners will receive appropriate online safety education to help them understand the safe use of ICT both in and out of school. Parents may find the Know IT All website (https://www.childnet.com/parents-and-carers) useful.

A full copy of the School's Online safety Policy (including all acceptable use policies) is available from the School Website or upon request from the school office.

Yours Sincerely,

Mrs Emily Massey

School Principal

Photos & Videos of Pupils taken at The Mendip School

The use of images and video plays an important part in learning at The Mendip School.

Students and members of staff may use digital cameras in lessons and to record evidence of learning, achievement and progress in lessons in and out of school. These images may then be used in presentations in subsequent lessons.

The school will comply with the Data Protection Act and GDPR Act and request parents / carers permission before publishing images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents and Carers are required to abide by the school's guidelines in the Online safety policy (available from the school website or on request) when taking digital images at, or of, school events and when using digital images which include images of other children.

Parents and Carers are requested to sign the permission form below to allow the school to publish images of their children.

Photos & Videos Permission Form

Parent / Carers Name .....

Student Name .....

As the parent / carer of the above pupil, I agree to the school publishing images of my child/children. I understand that the images in publicity that reasonably celebrates success and promotes the work of the school.

Signed ..... Date ……..

Additional Policies

School 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 South West Grid for Learning (SWGfL) 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 Network Manager. 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. These record and Logs are maintained on the SWGfL Filtering Site

To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL / school filtering service must:

- Be logged in change control logs
- Be reported to the ICT Coordinator

All users have a responsibility to report immediately to the Network Manager 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 / students will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). 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 online safety awareness sessions / newsletter etc.

Changes to the Filtering System

The Network Manager is responsible for changing and recording change to the Schools filtering systems.

Where the Network Manager feels that a request may violate or bypass existing filtering policies the request will be passed onto the Senior Management Team.

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 (the Network Manager who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the Network Manager can change this in the filtering management software, or by requesting a change with SWGfL.

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 Online safety Policy and the Acceptable Use agreement.

Audit / Reporting

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

- The Designated Safeguarding Lead
- The Network Manager
- The ICT Coordinator
- Members of SMT with the head teacher's approval
- SWGfL / 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.

School Password Security Policy

Introduction

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

• users can only access data to which they have right of access
• 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 Network Manager.

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the Network Manager. Any changes carried out must be notified to the manager of the password security policy (above).

Users will change their passwords every 30 Days

Training / Awareness

It is essential that 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 online 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 online safety lessons (the school should describe how this will take place)
- Through the Acceptable Use Agreement

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 Network Manager and will be reviewed at least annually.

All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

- Passwords must be changed every 30 days
- The last five passwords cannot be re-used
- The password should be a minimum of 8 characters long and
- Must include three of – uppercase character, lowercase character, number, special character
- The account will be "locked out" following 50 successive incorrect log-on attempts
- Temporary passwords are set to a formula and remain the same.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user

The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in the school safe, located in the Black files room.

The Network Manager will ensure that full records are kept of:

• User Ids and requests for password changes
• User logons
• 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 and stored in a secure manner.

These records will be reviewed by the ICT Co-ordinator.

This policy will be regularly reviewed in response to changes in guidance and evidence gained from the log.

School Personal Data Handling Policy

Recent publicity about the loss of personal data by organisations and individuals has made this a current and high profile issue for schools and other organisations. It is important that the school has a clear and well understood personal data policy because:

- No school or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school will want to avoid the criticism and negative publicity that could be generated by any loss of personal data.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is addressed by the UK Data Protection Act 1998 and following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that they adopt these procedures too.

It is important to stress that the Personal Data Policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. As it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

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 – Sept 2008).
It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot 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 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 "Fair Processing Code" 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 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, student progress records, reports, references
- 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

Responsibilities

The school's Bursar and Network Manager 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

• be the Information Asset Owners (IAOs)

The IAOs 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

Schools are recommended to adopt the SIRO and IAO positions in the Becta document – "Good Practice in information handling in schools ... " – see further reading section at the end of this template document.

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

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.

Information to Parents / Carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the school will inform parents / carers of all students of the data they hold on the students, the purposes for which the data is held and the third parties (e.g. LA, DCSF, QCA, Connexions etc) to whom it may be passed. This fair processing notice will be passed to parents / carers through the Parental AUP. Parents / carers of young people who are new to the school will be provided with the fair processing notice through the Parental AUP.

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: (schools should amend or add to as necessary)

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners (or insert titles of relevant persons)

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.

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: (the table below is taken from Becta guidance. Schools will need to decide, in line with LA Guidance how their data is marked)

[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

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 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 through the schools office 265 accounts which 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 fifteen 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 (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 data must be securely deleted from the device, in line with school policy (below) 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 to deal with Subject Access Requests ie. 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.

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. (see earlier section – LA / school policies may forbid such transfer)
- 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. (nb. to carry encrypted material is illegal in some countries)

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 (see further reading section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by the Network Manager.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- A "responsible person" for each incident
- A communications plan, including escalation procedures
- And results in a plan of action for rapid resolution and
- A plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further reading
Teachernet – Data processing and sharing -
http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/
Office of the Information Commissioner website:
http://www.informationcommissioner.gov.uk
Office of the Information Commissioner – guidance notes: Access to pupil's information held by schools in England
Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and it's four detailed appendices: (September 2008)
http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf
http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf
http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf
http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf
http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf
Cabinet Office – Data handing procedures in Government – a final report (June 2008)
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx