Bassenthwaite School
E-Safety Policy

Introduction

This E-Safety Policy should be considered with regard to all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks."

The policy also forms part of the school's protection from legal challenge, relating to the use of ICT.

School E-Safety Policy

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 *pupils / pupils* 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.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help 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 and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils / pupils 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 or inappropriate images or other 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
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' / pupils' 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 school must 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 e-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, pupils / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place 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 e-safety behaviour that take place out of school.

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 Health and Safety *Sub 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/CP Governor*. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- 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 is 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 Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Governing body will receive regular monitoring reports from the E-Safety Co-ordinator .
- The Headteacher and another member of the Senior Leadership 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.

E-Safety Coordinator / Officer:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends relevant meeting / committee of Governors

Network Manager / Technical staff:

The Network Manager / Systems Manager / ICT Technician /ICT Co-ordinator 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 e-safety technical requirements outlined in the 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, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 /Headteacher /ICT Co-ordinator / Class teacher
- that monitoring software / systems are implemented and updated as agreed in school policies

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 / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with pupils / 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 / pupils understand and follow the school e-safety and acceptable use policy
- 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 / 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

Pupils / pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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.

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 parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users (If the school should decide to use ICT equipment as part of the extended schools provision)

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – pupils / pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

- Pupils / 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 / pupils 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
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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, VLE
- Parents evenings

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:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

It is expected that some staff will identify e-safety as a training need within the performance management process.

- 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 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 meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / 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 training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the 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 be provided with a username and password by **Keswick School Primary ICT technician** who will keep an up to date record of users and their usernames.
- 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 a secure place (eg school safe)
- 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 CLEO
- Any filtering issues should be reported immediately to CLEO.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly 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
- 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.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up to date virus software.

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 / 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 / pupils 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.
- Pupils / 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 / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils / 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 / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- 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 should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils / 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 / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers is obtained as part of the AUP signed by parents or carers at the start of the year before photographs of pupils / pupils are published on the school website

Data Protection

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

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

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.

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				Pupils / 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	X							X
Use of mobile phones in lessons			X					X
Use of mobile phones in social time	X							X
Taking photos on mobile phones or other camera devices				X				X
Use of hand held devices eg 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		

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 / pupils should therefore use only the school email service to communicate with others when in school.
- 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 / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. ***These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging***

or public chat / social networking programmes must not be used for these communications.

- Pupils / 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.

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:

User Actions		Acceptable	Acceptable	Acceptable	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, eg 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 (eg financial / personal information, databases, computer / network access codes and passwords)					
Creating or propagating computer viruses or other harmful files					
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					

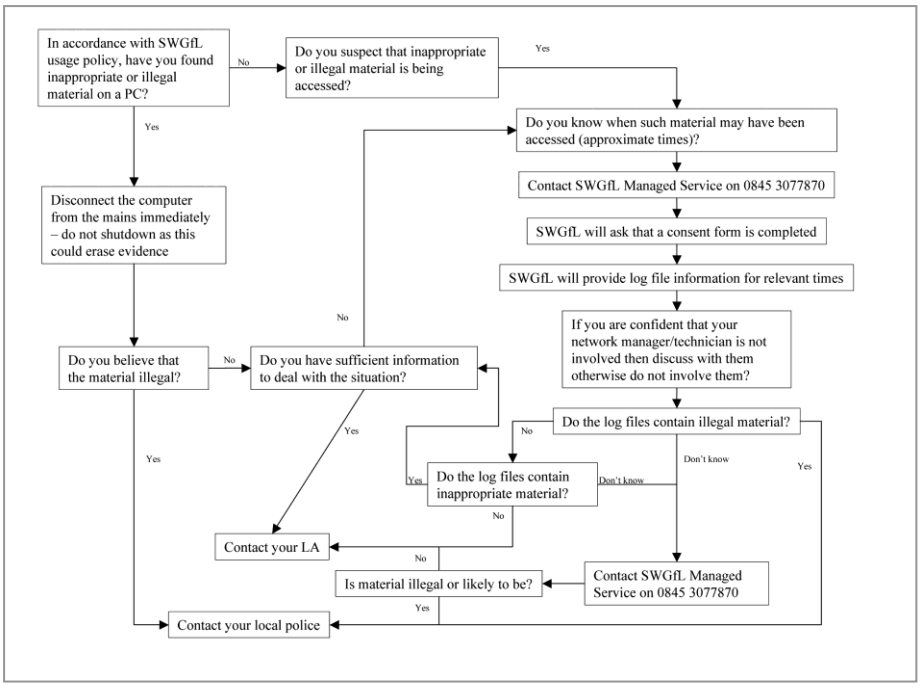
Responding to incidents of misuse

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 ie.

- **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 – 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 normal behaviour / disciplinary procedures as follows: √

Pupils / Pupils 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 /	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).		√	√	√					
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			√		√		√		
Attempting to access or accessing the school network, using another student's / pupil's account			√		√		√		
Attempting to access or accessing the school network, using the account of a member of staff			√		√		√		
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									
Using proxy sites or other means to subvert the school's filtering system			✓		✓		✓		
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			✓	✓					✓

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	RRefer 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 eg 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 pupils / 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								
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓		
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								✓

Date on which policy was approved 15/03/18

Policy review date: March 2020.....

Chair of Governors ------ M Taylor----------