St Hilary School
E-Safety Policy

Roles and Responsibilities

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

Headteacher, Governors and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. Please see the flow chart on dealing with e-safety incidents.
- The Headteacher or senior leaders will report any discrepancies to the relevant E safety Governors committee / meeting (Personnel, leadership and safeguarding).
- The Headteacher or senior leaders will ensure that children are safe from terrorist and extremist material when accessing the internet in school and that the school will equip children to stay safe online, both in school and outside. WRAPs training for ALL staff will ensure that staff are aware of the risks posed by the online activity of extremist and terrorist groups.
- The governors are responsible for monitoring e-safety in the school.

E-Safety Coordinator

- 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 school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety team to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team
- will monitor improvement actions identified through use of the 360 degree safe self-review tool with support from the e safety governor

Technical staff:

The Systems Manager ICT4 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 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 they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator

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/ Headteacher / Senior Leader

- digital communications with pupils (email) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extracurricular and extended school activities.
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection

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:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and 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 and information about national and local e-safety campaigns. Parents and carers will be responsible for:

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

Education – pupils

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

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

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. E-safety is embedded in the termly units of the Computing curriculum.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / 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
- Students / 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
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be explained and displayed when necessary.
- 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, website
- Parents evenings arranged
- Reference to the CEOPs website

Education - Extended Schools

The school will offer e-safety meetings so that parents and children can together gain a better understanding of these issues. 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.

Radicalisation

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content.

We also filter out social media, such as Facebook. Searches and web addresses are monitored and the ICT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Where staff, students or visitors find unblocked extremist content they must report it to a senior member of staff.

We are aware that children and young people have access to unfiltered internet when using their mobile phones and staff are alert to the need for vigilance when pupils are using their phones.

The Acceptable Use of ICT Policy (AUP) refers to preventing radicalisation and related extremist content. Pupils and staff are asked to sign the AUP annually to confirm they have understood what is acceptable.

Pupils and staff know how to report internet content that is inappropriate or of concern.

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.
- 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 will receive regular updates through attendance at SWGfL / LA and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice and 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 subcommittee / 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 National Governors Association / SWGfL or other relevant organisations.
- Participation in school training / information sessions for staff or parents.
- Will support the e safety co-ordinator with the 360 degree self-evaluation tool.

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 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 guidance. The systems will also ensure that our duty to ensure that children are safe from terrorist and extremist material is upheld.
- 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, at least annually, by the E-Safety co-ordinator/Senior leader. There are separate rights for senior leaders, staff and children.
- All users will be provided with a username and password by the network Manager who will keep an up to date record of class users and their passwords. There are class log ons, and although the school understands the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP, the pupils are always supervised while they are accessing the internet. Members of staff should never use a class log on for their own network access.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher/ Senior leader and kept in a secure place
- 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 service provided by 'Smoothwall'.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately to the headteacher or senior leader who will the inform Smoothwall.
- 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.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager. Any incident will be reported to the E safety co-ordinator who will follow the SWGfL flow chart.
- ICT 4 have appropriate security measures 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" onto the school system. Any guests will be given a temporary password to access the school system.
- An agreed policy is in place regarding the downloading of executable files by users. Only the administrator can install these files.
- An agreed policy is in place that allows staff to install programmes on school workstations portable devices. Only programs that have been agreed by the Senior leaders/ E safety supervisor/ Network manager will be allowed onto the workstations.

- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. In no circumstances should pupil personal data/photographs with names be saved onto removable media.
- 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.

Curriculum

E-safety should be a focus in all areas of the curriculum and will play an important part in equipping children and young people to stay safe online, both in and outside of school. E-safety sessions will take place at least termly but internet safety will be embedded in PSHE and SRE. General advice and resources for schools are available on the UK Safer Internet Centre Website.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- All teachers will receive WRAP training, which will highlight the risks posed by the online activity of extremist and terrorist groups.
- Where 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 should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil's instant use of images that they have recorded themselves or downloaded from the internet. No images taken by individuals will be allowed to be published or put onto the internet unless permission is granted from the parents or from the e safety co-ordinator.

- When using digital images, staff should inform and educate students / 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 are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of 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.
- Transfer data using encryption and secure password protected devices.

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

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

Social Media protecting professional Identity

With an increase in use of all types of social media for professional and personal purposes the school has a social network policy a policy that sets out clear guidance for staff.
The school has a duty of care to provide a safe learning environment for pupils and staff. The school could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

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

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school.*

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.

	Staff & other adults				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 and handed to the teacher.	X						x	
Use of mobile phones in lessons See notes below for teachers		x						x
Use of mobile phones in social time	x							x
Taking photos on school camera devices	x						x	
Use of electronic devices, iphones, ipads		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 MSM				x				x
Use of social networking sites				x				x
Use of blogs		x					x	

The use of mobile phones by teachers is only allowed when permission is granted by the Head teacher for personal reasons. They should not be used for texting, phoning, photographs or any other use during class time.

User Actions

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	
Use of video broadcasting eg Youtube	

Responding to incidents of misuse

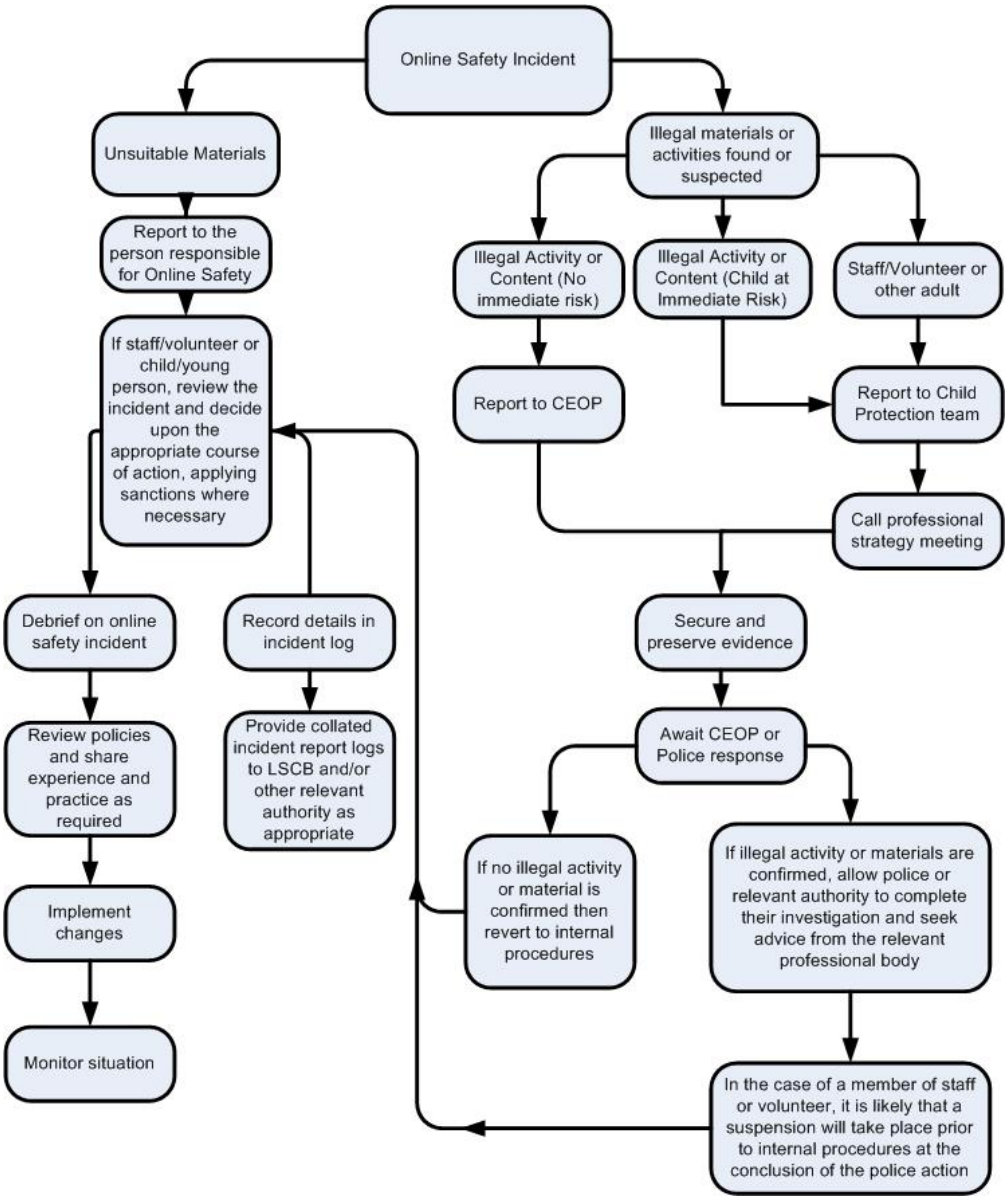
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the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

Illegal Incidents

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



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:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Headteacher	Inform parents / carers	Refer to technical support staff of r action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion	Refer to Police	
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	X	X							
Unauthorised use of mobile phone / digital camera / other handheld device	X	X	X						
Unauthorised use of social networking / instant messaging / personal email	X	X	X	X					
Unauthorised downloading or uploading of files	X	X	X	X					
Allowing others to access school network by sharing username and passwords	X	X							
Attempting to access or accessing the school network, using another student's / pupil's account	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				
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		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X				
Deliberately accessing or trying to access offensive or pornographic material	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	

Staff

Incidents:	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	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 or attempting to access or accessing the school network, using another person's account	X				X		
Careless use of personal data eg holding or transferring data in an insecure manner	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
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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	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
Using proxy sites or other means to subvert the school's filtering system(without permission)	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
Breaching copyright or licensing regulations	X	X	X		X	X	X

Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X

Signed by Headteacher: K Butcher

Date:

Signed by Chair of governors: Mr D Sharp

Date:

To be reviewed: Autumn 2021