Sherington Primary School E-Safety Policy

Ofsted describes e-safety as a school's ability to protect and educate pupils and staff in their use of technology as well as having appropriate mechanisms in place to intervene and support any incident where appropriate.

At Sherington we take the safeguarding of pupils and staff seriously. We work to ensure that we are helping to create safer environments for pupils, staff and families on-line as well as off.

Enabling pupils to take full advantage of technology and preparing them for the real world whilst providing a safe environment is a tricky balancing act. Locked-down systems that exert total control over what students can access online provides no opportunity for them to learn how to become digitally responsible.

Protecting student's - means providing a safe learning environment by using appropriate monitoring and filtering to control what pupils can access while at school. But, this only protects them while they are on school premises. Education around e-safety is the only way to ensure that, wherever they are, they know how to stay safe online.

As a learning community, the school works in conjunction with parents to educate and safeguard pupils and families.

Educate:

•Online behaviour – understanding what constitutes cyber-bullying, how to behave safely and show respect for others

•Protecting your online reputation – understanding the risks and rewards of sharing personal information online (your digital footprint)

•Rules and regulations around social networking

•Understanding the reliability and validity of online information

•Data security – keeping your personal information safe and being aware of viruses and hacking

•Knowing what to do if anything bad happens

Scope

This policy applies to all members of the school community who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers headteachers to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which takes place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and will inform parents/carers of incidents of inappropriate e-safety behaviour.

Roles and Responsibilities

Governors:

- Are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy

Headteacher & Senior Leaders:

- Have a duty of care for ensuring the safety (including e-safety) of members of the school community

- Senior leaders should be aware of procedures to follow in the event of a serious safety allegation being made against a member of staff
- The headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff suitable training to enable them to carry out their e-safety roles and to train others
- 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

E-Safety Co-ordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policy
- 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, support and advice
- Liaises with LA and relevant bodies
- Liaises with technical staff/support
- Attends relevant meetings
- Reports regularly to SLT

Technical Support (under guidance of Computing Lead):

- Ensures that the school's technical infrastructure is secure and not open to misuse or malicious attack
- Ensures that the school meets required e-safety technical requirements or any LA guidance that may apply
- Ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Ensures that filtering is applied and updated regularly

- Keeps up-to-date with technical information in order to effectively carry out their role and to inform and update others
- Ensures that the use of the network/internet/email is regularly monitored in order that misuse/attempted misuse can be reported

Teaching & Support Staff:

Are responsible for ensuring that...

- They are aware of e-safety matters and current policy/practice
- They have read, understood and signed Acceptable Use Policy
- They report suspected misuse or problems to the Headteacher for investigation
- All digital communication with students/pupils/parents/carers should be on a professional basis
- E-Safety issues are embedded in all aspects of the curriculum
- They monitor the use of digital technologies and implement current polices when using 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 Safeguarding Person:

Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues that arise from:

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

Parents/Carers:

- Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:
- Digital and video images taken at school events
- Access to parents sections of the website
- Their children's personal devices in their school (where this is allowed)

Community Users:

- Community users who access school systems/website as part of the wider school provision will be expected to sign a Community User Agreement before being provided with access to the system

Policy Statements

Education - Pupils

Whilst regulation and technical solutions are 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 resilience.

E-safety should be a focus in all aspects of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad and relevant. Providing opportunities for progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided a part of Computing/PSHE/other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils 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
- Pupils should be taught to acknowledge the source of information used to respect copyright when using material accessed on the internet

- Pupils should be helped to understand the need for the pupils Acceptable Use Agreement and encouraged to adopt a safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where the 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of websites visited
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination etc.) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study

Education – Parents/Carers

Many parents/carers have only 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 online behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, school website

- Parents/carer evenings/sessions
- High profile events/campaigns (i.e. Safer Internet Day)
- Reference to relevant websites/publications

Education – Wider Community

The school will provide opportunities from time to time for families to gain from the school's e-safety knowledge and experience. This may be offered through:

- Providing family learning courses in the use of new digital technologies, digital literacy and e-safety
- E-safety messages targeted at other family members beyond just parents i.e. Grandparents
- The school website will provide e-safety information for the wider school community

Education & Training – staff/volunteers

It is essential that all staff receive e-safety training and understand their responsibilities. Training will be offered as:

- A programme of formal e-safety training will be made available to all staff
- An audit of the e-safety needs of all staff will be carried out regularly to inform training
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the e-safety policy and Acceptable Use Agreements signed
- The e-safety lead will receive regular updates through attendance at external training events and by reviewing guidance documents
- The e-safety policy is presented/shared with staff

Training – Governors

Governors should take part in e-safety training/awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the LA/National Governors Association or relevant organisation
- Participation in school training/information sessions

Technical Infrastructure – Equipment, Filtering, Monitoring

The school will be responsible for ensuring that the school infrastructure/network is safe and secure.

- School systems will be managed in ways that ensure the school meets recommended requirements
- There will be regular reviews and audits of the safety and security of school systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- The headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users
- Technical staff monitor and check the activity of users
- Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts threaten the school's security
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted

Use of Digital and Video Images

Technological advances allow staff and pupils instant use of images that they have recorded/produced themselves or down-loaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images might for example provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment. It is common for perspective employers to carry out internet searches for information about potential or existing employees. Therefore the school has a responsibility to educate users about the risks and should implement policies to reduce the likelihood of the potential for harm:

- When using digital images staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect privacy and in some cases protection these images should not be published or made publicly available on social networking sites
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images which should only be taken on school equipment; personal equipment 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 includes pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupil's full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents and carers will be obtained before photographs of pupils are published on the school website or twitter

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

The school must ensure:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without necessary delay

- All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing'
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear/understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office

Staff must ensure they:

- 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

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 the risks/disadvantages:

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

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. User should be aware that

email communications are monitored. Staff and pupils should therefore only use the school email service to communicate with others when in school, or on school systems

- Users must immediately report, to the nominated person – in accordance with policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students, pupils or parents/carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Whole class/group email addresses many be used at KS1, while students at KS2 will be provided with individual school email addresses for educational use
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media – Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or

disability or who defame a third party may render the school 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

Staff should ensure that:

- No reference should be made in staffs personal social media to pupils, parents/carers or other 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss personal information

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the other policies.

School's Twitter Account

This will be used as a whole school communication tool to engage with parents about the activities and learning experiences that are happening in school.

Twitter is web-based application we adopt the same rules for our school's Twitter account as we do for our school website. Where the parents do not wish their child's image to appear on the school's website or on Twitter, the school will aim to follow these wishes.

Please note the following that is appropriate for staff using the schools twitter account:

1. I will never be derogatory to any person or bring the school name into disrepute.
2. I will never engage knowingly with a pupil outside of school.
3. I will not engage with parents via this account
4. I will retain a professional boundary at all times.
5. I am aware of the student's in my class that do not have parental consent to use their picture on the website or twitter
6. I will never refer to names of students at any time

Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school

or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	pornography			X	
	promotion of any kind of discrimination			X	
	threatening behaviour, including promotion of physical violence or mental harm			X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	

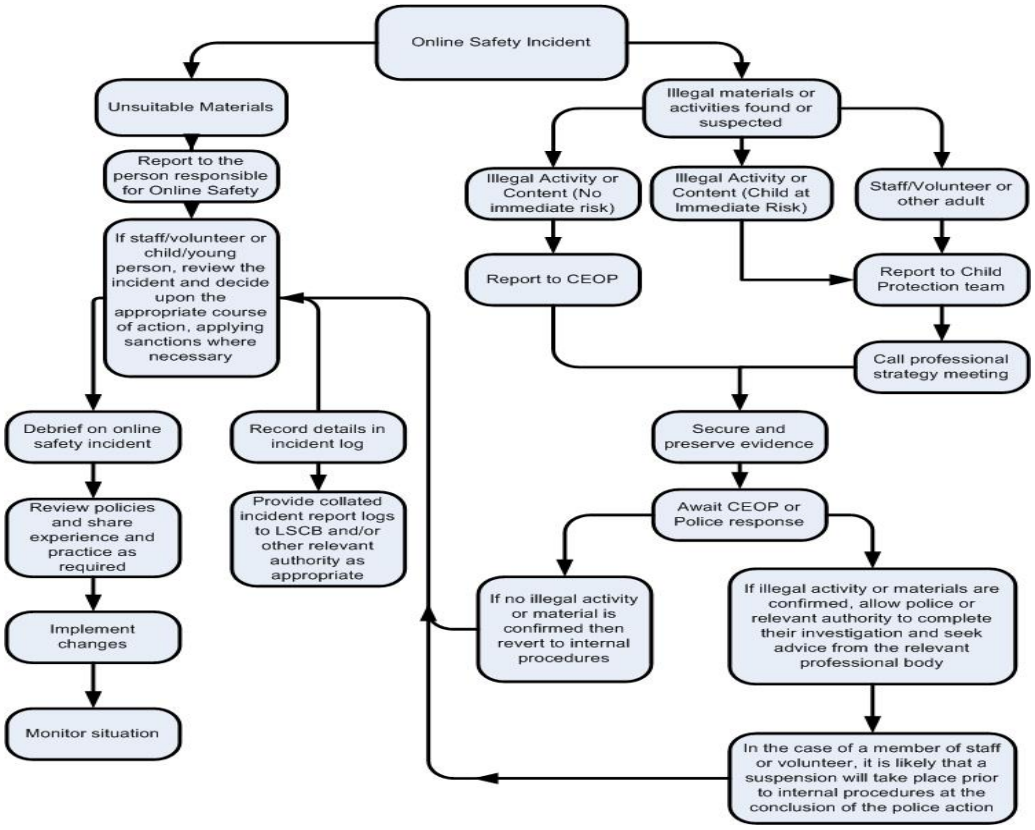
On-line shopping / commerce		X		
File sharing		X		
Use of social media		X		
Use of messaging apps			X	
Use of video broadcasting eg Youtube	X			

Responding to Incidents of Misuse

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

Illegal Incidents

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



Other Incidents

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

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

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

  - Involvement by the Local Authority or national/local organisations (as relevant)
  - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
  - Incidents of grooming behaviour
  - The sending of obscene materials to a child
  - Adult material which potentially breaches the Obscene Publications Act
  - Criminally racist material
  - Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

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

School Actions & Sanctions

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

Students / Pupils

Incidents:	Refer to class teacher	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
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	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	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system					X		X	
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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		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	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
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	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	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		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
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X

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