Sunningwell C of E Primary School

Online Safety Policy Sept 2019

Development of this Policy

This online policy has been developed by the headteacher supported by staff and governors. Consultation with parents and carers has been sought through Parentmail. It has been updated to reflect the General Data Protection Regulations 2018.

Schedule for Development / Monitoring / Review

This online policy was approved by the *Governing Body*	
The implementation of this online policy will be monitored by the	*Headteacher*
Monitoring will take place at regular intervals:	*Annually*
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online or incidents that have taken place. The next anticipated review date will be:	
Should serious online incidents take place, the following agencies should be informed:	*LADO or Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring by teaching staff

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents and carers and visitors) who have access to and are users of school IT systems.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, 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 online-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about any online incidents and monitoring reports.

Headteacher and Senior Leaders:

- The headteacher has a duty of care for ensuring the safety (including online) of members of the school community, though the day to day responsibility for online activity may be delegated to a member of staff.
- The Headteacher and the deputy head are aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff (see flow chart on dealing with online incidents page 8).
- The headteacher, deputy and other members of staff have been trained in online safety.

- The headteacher will ensure that governors monitor and support those in school who carry out the internal online monitoring role.
- The headteacher will receive regular monitoring reports from the staff.
- The headteacher takes day to day responsibility for online issues and has a leading role in establishing and reviewing the school online policies
- The headteacher ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- The headteacher provides training and advice for staff
- The headteacher liaises with the Local Authority/relevant body as needed
- The headteacher liaises with school technical staff
- The headteacher receives reports of online incidents which should include a log of incidents in the behaviour folder in the staffroom to inform future online developments.

123ICT is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online technical requirements and any Local Authority Online Policy or Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.
- the 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 online technical information in order to effectively carry out their online role and to inform and update others as relevant
- that the use of the network, internet, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation
- that monitoring software and systems are implemented and updated as needed to provide a safe online environment for the school

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current online policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher
- all digital communications with pupils, parents and carers should be on a professional level
- online issues are embedded in all aspects of the curriculum and other activities
- online pupils understand and follow the online and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current 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

Safeguarding Designated Lead (headteacher)

The headteacher is trained in online issues and aware of the potential for serious child protection/safeguarding issues that might arise from:

- sharing of personal data
- access to illegal and/or inappropriate materials
- inappropriate on-line contact with adults and/or strangers
- potential or actual incidents of grooming
- online-bullying

Pupils, where age appropriate:

- are responsible for using the school's digital technology systems 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 and use of images and on online-bullying.
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's Online Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the website and information about national and local online campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Policy Statements

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 online safety is therefore an essential part of the school's online provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing, PHSE and other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials and 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
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and be encouraged to adopt safe and responsible IT 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 internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents and Carers

Many parents and carers have only a limited understanding of online risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people 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:

- newsletters, Parentmail and the website
- Parents/Carers evenings sessions

Education & Training – Staff and Volunteers

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

- A planned programme of formal online training will be made available to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly.
- All new staff should receive online training as part of their induction programme, ensuring that they fully understand the school online policy and Acceptable Use Agreements.)
- This Online policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

Training – Governors

Governors should take part in online training sessions, with particular importance for those who are members of any sub-committee involved in technology, online, health and safety or child protection. This will be offered by participation in school training and information sessions for staff or parents.

Technical – infrastructure and equipment, filtering and monitoring

123ICT as technical support provider for Sunningwell C of E Primary 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. 123 ICT will also need to ensure that the relevant people in school will be effective in carrying out their online responsibilities:

- The school's technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to the school's technical systems and devices.
- All users at KS2 and above will be provided with a username and secure password by *Mrs Louise Plumb who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password group or class log-ons and passwords may be provided for KS1 and below.
- The "master administrator" passwords for the school's ICT system, used by the Network Manager must also be available to the *Headteacher and Mrs Louise Plumb* and kept in a secure place.
- Mrs Louise Plumb 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 by EXA Net-works Surfprotect (supported by 123 ICT).
- Appropriate security measures are in place through the use of Sophos Anti-virus software to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published ormade publicly available on social networking sites, nor should parents or carers comment on any activities involve pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must take care 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.
- 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 current data protection legislation.

The school will ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- 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 for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- The school will have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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, memory 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.

Communications

Children should not bring mobile phones or digital recording equipment into school. They may be used on school trips under the responsibility of the child but any images/videos must not be posted online or shared without the permission of any child included in the video/images.

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. Users should be aware that email communications are monitored.
- Users must immediately report, to the headteacher, 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 pupils or parents and carers 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.
- pupils should be taught about online 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* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made in social media to 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

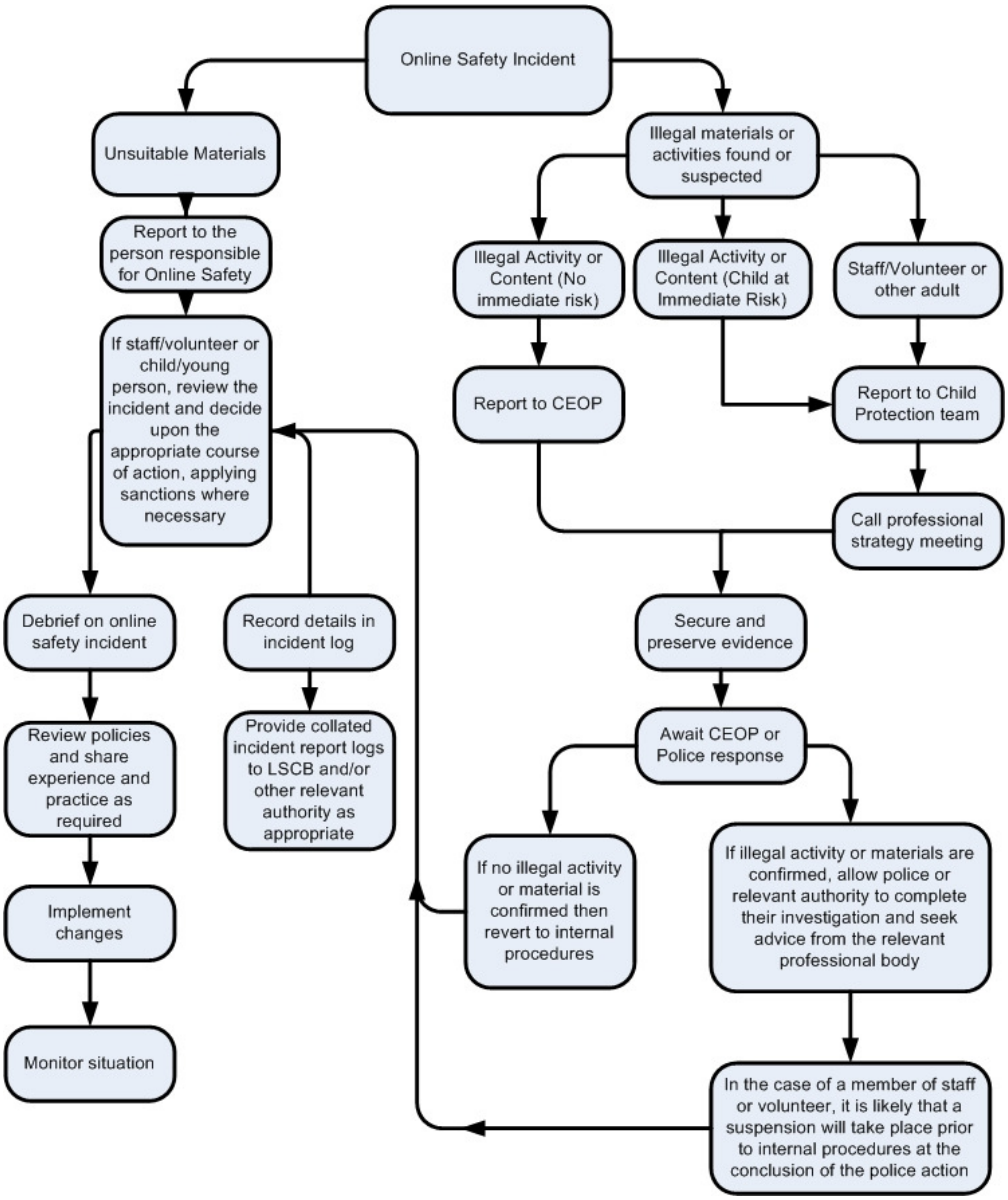
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse 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 /					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 use when staff members 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 the right hand side of the Flowchart (below and appendix) 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 users 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/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure 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 of the content 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 Local Authority or national / local organisation (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 dealt with through normal behaviour/disciplinary procedures as follows:

Incidents Pupils:	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					X
Unauthorised use of non-educational sites during lessons	X						X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X				X		X	X
Unauthorised use of social media / messaging apps / 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		X		X			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
Corrupting or destroying the data of other users		X		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
Continued infringements of the above, following previous warnings or sanctions		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
Using proxy sites or other means to subvert the school's / 's filtering system		X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X	X		X

Incidents:	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	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			
Inappropriate personal use of the internet /social media /personal email	x				x	x
Unauthorised downloading or uploading of files	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					
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
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software					x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x				x	x
Using personal email /social networking /instant messaging /text messaging to carrying out digital communications with students /pupils	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	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	x		x	x
Breaching copyright or licensing regulations	x				x	x
Continued infringements of the above, following previous warnings or sanctions	x				x	x

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:
http://www.swgfl.org.uk/Staying-Safe/Creating-an-Online-policy

Acknowledgements

Sunningwell School has adapted and adopted the policy of SWGfL. They would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Policy Template and of the 360 degree safe Online Self Review Tool:

- Members of the SWGfL Online Group
- Representatives of SW Local Authorities
- NEN / Regional Broadband Grids
- Avon and Somerset Police
- Plymouth University Online Safety