



# Online Safety Policy

Review date: January 2022

[Review of this Policy](#)

This East-the-Water Online Safety policy has been developed by key staff members including:

- Headteacher
- Senior Leadership Team
- Staff – including Teachers, Technical staff
- Governors
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

## Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body	
The implementation of this Online Safety policy will be monitored by the:	Senior Leadership Team
Monitoring will take place at regular intervals:	Once a year
The Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Once a year
The Online Safety 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 Safety or incidents that have taken place. The next anticipated review date will be:	January 2022
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, Police

We will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
  - pupils
  - parents / carers
  - staff

## Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of our school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

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

## Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

## Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents. A member of the Governing Body Board has taken on the role of Online Safety Governor ([it is suggested that the role may be combined with that of the Child Protection / Safeguarding Governor](#)). The role of the Online Safety Governor will include:

- regular monitoring of Online Safety incident logs
- reporting to relevant Governors
- Regular meetings with online safety coordinator

## Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Senior Leaders are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The 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 Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

## Online Safety Coordinator:

- leads the Online Safety committee
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff through the Boost training system
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- attends relevant meeting of Governors
- reports regularly to Senior Leadership Team

## ICT Co-ordinator and Technical staff:

Are 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 Safety technical requirements and any Local Authority Online Safety Policy Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network and internet is regularly monitored in order that any misuse can be reported to the Online Safety Coordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

## Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Online Safety Coordinator for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety and acceptable use policies
- 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 students 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
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

## Safeguarding Officer:

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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

## Students / pupils:

- are responsible for using the school digital technology systems safely as taught through lessons and addressed in this policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so through the school's reporting systems
- 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 and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

## 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 and the school website. Parents and carers will be encouraged to support the school in promoting good Online 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 the school (where this is allowed)

## Community Users

Community Users who access school systems provision will be expected to sign a Community User AUA before being provided with access to school systems.

# 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 to their own use of computer systems both in and out of school. The education of pupils in Online Safety is therefore an essential part of our school's Online Safety provision.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety 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 will be provided as part of Computing and PHSE and should be taught half-termly.
- Key Online Safety messages are reinforced as part of a planned programme of assemblies.
- Pupils will 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 will be helped to understand the need for safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- Pupils must not use devices such as laptops and Ipads unsupervised.
- In lessons where internet use is pre-planned, it is best practice that pupils are 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.
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

## Education – parents / carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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
- School website
- Parents evenings
- Leaflets and handouts

## Education & Training – Staff / Volunteers

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

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
- All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Coordinator will provide advice, guidance and training to individuals as required.

## Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of Online Safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation
- Participation in school training / information sessions for staff or parents

## Technical – infrastructure / equipment, filtering and monitoring

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

- School 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 academy technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users will have clearly defined access rights to school's technical systems and devices.
- All users will be provided with a username and secure password by the school ICT technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Pupils will also have their own class logins with restricted access.
- The “ administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place
- The school ICT technician 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place 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 and all staff laptops are encrypted for protected use off the school site.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / 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 cyberbullying 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. 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 / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- 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. 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 from those who have the adequate permission to do so.

- 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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to current data protection update which states that personal data must be:

- 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.
- There is 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. (many memory sticks / cards and other mobile devices cannot 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 / academy policy (below) once it has been transferred or its use is complete.

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how our school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
<b>Communication Technologies</b>								
Mobile phones may be brought to school		✓: 0 ✓						✓
Use of mobile phones in lessons				✓				✓ ✓
Use of mobile phones in social time				✓ ✓ ✓	✓			✓
Taking photos on mobile phones or personal devices				✓				✓
Use of other mobile devices eg 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			✓					✓ ✓ ✓

## Unsuitable / inappropriate activities

At East-the-Water we believe 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:

Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
				X

## User Actions

Users shall not visit Internet	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
--------------------------------	---	--	--	--	--	---



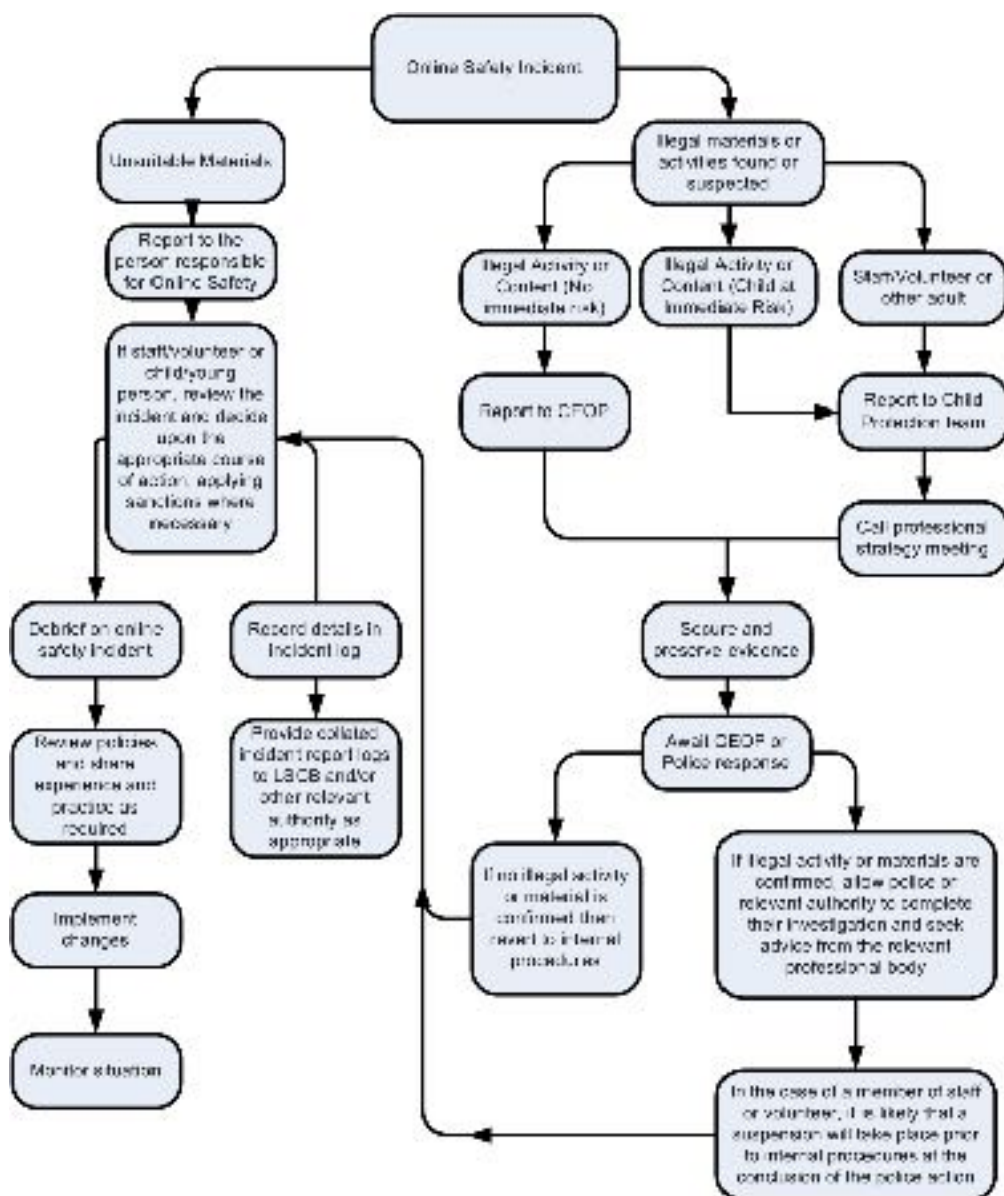
sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic 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 use 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 the 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 our school community will be responsible users of digital technologies, who understand and follow school / academy 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 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.
- 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 we as a school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

### Pupils

---

Incidents:	Refer to class teacher	Refer to E Safety Coordinator / ICT Co-ordinator	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 - 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	
Unauthorised use of social media / messaging apps / personal email			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
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	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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X		X	X

Staff

Actions / Sanctions

---

Incidents:	Refer to E Safety Co-ordinator / ICT Co-ordinator	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X			X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X			X	X	X
XUnauthorised downloading or uploading of files	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	X		X	X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X		X	X	X	X
Deliberate actions to breach data protection or network security rules	X	X	X	X		X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X		X	X	X
Sending an email, text or 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	X	X				X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	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	X	X

## Acknowledgements

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