H10 Online Safety Policy

Scope

The School is committed to promoting and safeguarding the welfare of all students and an effective online safety strategy is paramount to this. This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalisation happen through the online medium.

The aims of the School's online safety strategy are threefold:

1. To protect the whole School community from illegal, inappropriate and harmful content or contact;
2. To educate the whole School community about their access to and use of technology; and
3. To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).

This policy applies to all members of the School community including, but not limited to: staff and volunteers, students, parents and visitors, any individual who has access to the School's Technology whether on or off School premises, or otherwise use Technology in a way which affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

The following policies, procedures and resource materials are also relevant to the School's online safety practices:

- ICT Acceptable Use Policy for Students
- ICT Acceptable Use Policy for Staff
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Risk Assessment Policy for Student Welfare
- Staff Handbook

These policies, procedures and resource materials are available to staff on the staff shared drive, online staff handbook, and hard copies are available on request.

Roles and Responsibilities

The Governing Body

- The Governing Body as proprietor has overall responsibility for safeguarding arrangements within the School, including the School's approach to online safety and the use of technology within the School.

- The Governing Body is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of students. The adoption of this policy is part of the Governing Body's response to this duty.

- The Link Governor for Safeguarding is the senior board level lead with leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body.

- The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies.

Principal and Senior Leadership Team

- The Principal has overall executive responsibility for the safety and welfare of members of the School community.

- The Designated Safeguarding Lead (DSL) is a senior member of staff from the Senior Leadership Team (SLT) with lead responsibility for safeguarding and child protection. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Child Protection Policy.

- The DSL will work with the IT Manager (see below) in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of students.

- The DSL will regularly monitor any breaches of the school filtering and monitoring system and maintain a record of any sanctions or other interventions

- The DSL will regularly update other members of the SLT on the operation of the School's safeguarding arrangements, including online safety practices

IT Manager

- The IT Manager is responsible for the effective operation of the School's filtering and monitoring system so that students and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network or any school-managed devices

- The IT Manager is responsible for ensuring that:
    - the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
    - the user may only use the School's Technology if they are properly authenticated and authorised;
    - the School has an effective filtering policy in place and that it is applied and updated on a regular basis;
    - the risks of students and staff circumventing the safeguards put in place by the School are minimised;
    - the use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to

the appropriate person for investigation; and
    - monitoring software and systems are kept up to date to allow the IT Manager and Bursar to monitor the use of email and the internet over the School's network and maintain logs of such usage.

- The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

- The Bursar will report termly to the SLT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, s/he will escalate those concerns promptly to the appropriate member(s) of the School's Senior Leadership Team (SLT).

All Staff

- All School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with students.

- Staff are expected to adhere, as far as applicable, to each of the policies referenced in section 1.

- Staff have a responsibility to report any concerns about a student's welfare and safety in accordance with this policy and the School's Child Protection and Safeguarding Policy.

- Residential staff are encouraged to maintain extra vigilance on their use of the school network, including wireless access on personal devices, and ensure that they are not accessing inappropriate material whilst using the school infrastructure.

- All Staff must understand their responsibilities towards protecting children online and will be provided training as appropriate.

Parents

- The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:
    - support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;
    - talk with their child(ren) to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and
    - encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another student or need support.

- If parents have any concerns or require any information about online safety, they should contact their child's Houseparent in the first instance.

Education and Training

Students

- Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy).

- The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students:
    - about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;
    - to be critically aware of content they access online and guided to validate accuracy of information;
    - how to recognise suspicious, bullying, radicalisation and extremist behaviour;
    - the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
    - the consequences of negative online behaviour; and
    - how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

- The School's Acceptable Use of ICT Policy for Students sets out the School rules about the use Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology. Students are reminded of the importance of this policy on a regular basis.

- When the DSL observes a breach of policy, whether through an alert on the School's filtering and monitoring system or through a report from another member of staff, s/he will ensure that targeted interventions will take place as appropriate to educate students as to the dangers of their activity. This will usually be through the student's Houseparent in the first instance.

Staff

- The School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

- Induction training for new staff includes guidance on this policy as well as the Staff Handbook. Ongoing staff development training includes training on Technology safety together with specific safeguarding issues including cyberbullying and radicalisation.

- Staff also receive data protection guidance on induction and at regular intervals afterwards.

- The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

Parents

- Information is available to parents via the school website. Additionally, we offer the opportunity for parents to attend School based sessions on online safety on an annual basis.

- Parents are encouraged to read the Acceptable Use Policy for Students with their son/daughter to ensure that it is fully understood.

- It is important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the School (if anyone) their child is going to be interacting with online. Whilst this is most applicable in cases of online or remote learning where necessary, the increasing use of technology in the classroom and for homework and additional learning means that staff should be conscious of communicating with parents should there be any requirement to use technology whilst at home.

- The DSL will ensure that appropriate information and resources are made available to parents via newsletters and a dedicated area on the school website.

Useful Resources

There are useful resources about the safe use of Technology available via various websites including:

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.educateagainsthate.com
www.kidsmart.org.uk
www.safetynetkids.org.uk
www.safekids.com
www.parentinfo.org

DfE's Advice for head teachers and School staff on cyberbullying
DfE's Advice for parents and carers on cyberbullying
DfE's guidance on the use of social media for online radicalisation
DfE's Advice for teaching online safety in schools
DfE's guidance on Harmful online challenges and online hoaxes
UK Council for Internet Safety (UKCIS) guidance on Education for a connected world
UKCIS guidance on Sharing nudes and semi-nudes (advice for education settings)

Access to the School's Technology

The School provides internet and an email system to students and staff as well as other Technology including managed devices such as Chromebooks. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and Bursar.

Students and staff require individual user names and passwords to access the School's wireless network and to access the Google Suite which must not be disclosed to any other person. Any

student or member of staff who has a problem with their user names or passwords must report it to the IT Manager immediately. The school has implemented two-factor authentication for staff access to Google services as an additional layer of security.

No laptop, tablet or other mobile electronic device may be connected to the School network without the consent of the IT Manager. All devices connected to the School's network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the School's network will be logged and monitored by the IT Department.

The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

Use of Mobile Electronic Devices

- The School has appropriate filtering and monitoring systems in place to protect students using the Internet (including email text messaging and social media sites) when connected to the School's network. Mobile devices equipped with a mobile data subscription can, however, provide students with unlimited and unrestricted access to the internet. The school does allow students in Year 9 and above to carry their mobile devices with them at school but expect them to follow the Acceptable Use of Technology Policy for Students.

- The School rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Students.

- The use of mobile electronic devices by staff is covered in the Staff Code of Conduct.

- The School's policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

Procedures for Dealing with Incident of Misuse

Staff, students and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's Child Protection and disciplinary policies and procedures.

Misuse by Students

- Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

- Anyone who has any concern about the welfare and safety of a student must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy.

Misuse by Staff

- Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

- If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Child Protection Policy.

Misuse by Any User

- Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the IT Manager or the Principal.

- The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

- If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

Monitoring and Review

All incidents and breaches of policy involving the use of Technology will be logged centrally in the Student Incident Log by the DSL, or in the Staff Incident Log by the Bursar.

The DSL and SLT have responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.

Consideration of the effectiveness of the School's online safety procedures and the education of students about keeping safe online will be included in the Governors' annual review of safeguarding.

Dealing with Unsuitable / Inappropriate Activities

Some internet activity, for example accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities such as cyber-bullying would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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 / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

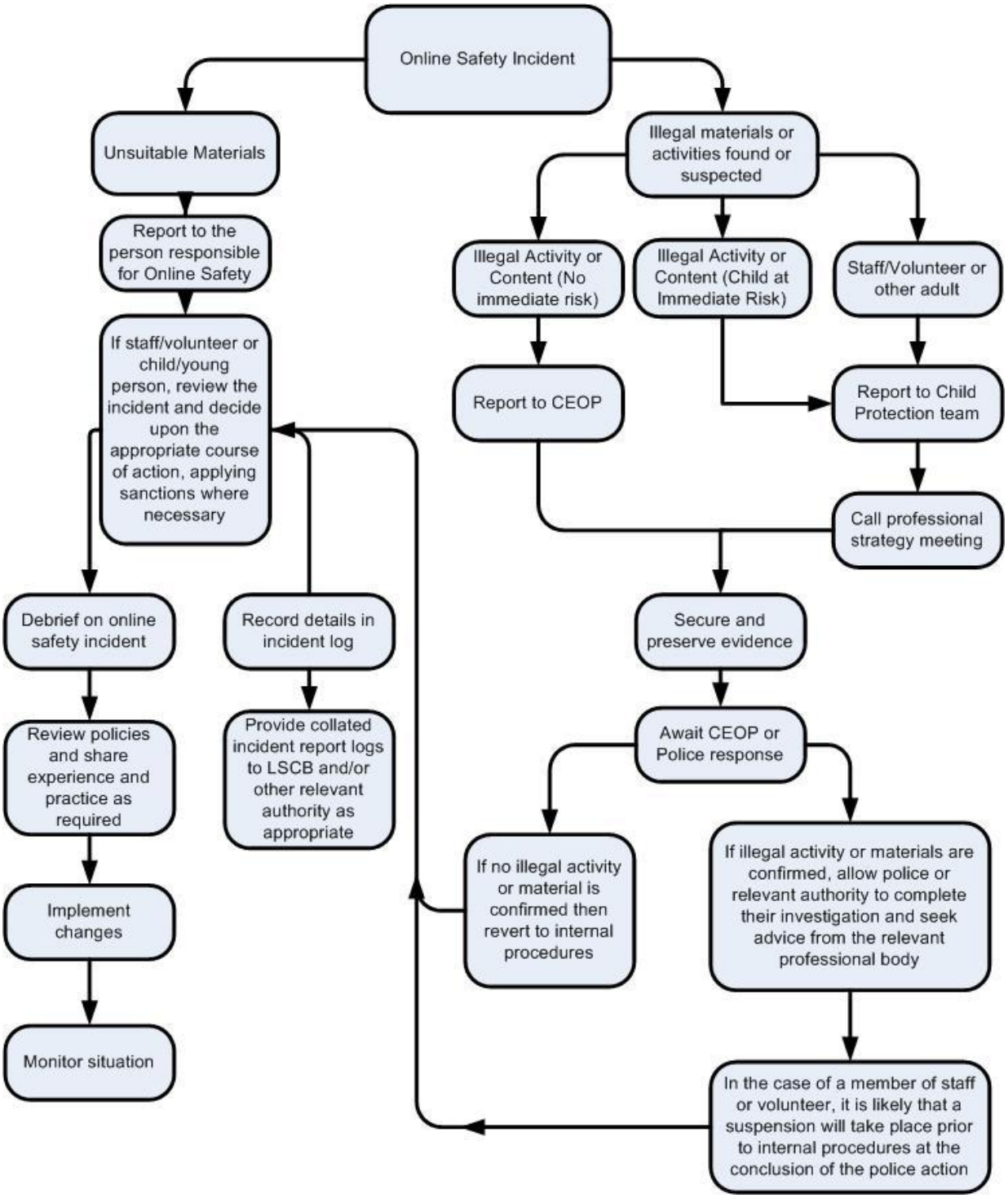
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain	Child sexual abuse 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
	Promotion of extremism or terrorism					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	

or relate to:						
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 (e.g. 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 (legal)			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. 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.

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.



(CEOP – Child Exploitations and Online Protection command)

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 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
    - 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
- promotion of terrorism or extremism
- 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and 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, these will be used as appropriate depending on the individual situation, some or all of the actions/sanctions marked maybe used:

	Actions / Sanctions								
Students Incidents	Refer to class teacher	Refer to Head of Department / House parent	Refer to Principal / SLT	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 e.g. 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	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X						X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X	X	X	X	X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files		X	X		X	X	X	X	X
Allowing others to access school / network by sharing username and passwords					X		X	X	

Attempting to access or accessing the school network using another student's account		X	X		X	X	X	X	X
Attempting to access or accessing the school network using the account of a member of staff			X		X	X	X	X	X
Corrupting or destroying the data of other users		X	X		X	X	X	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	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X	X	X	X
Actions which could bring the school / into disrepute or breach the integrity of the ethos of the school		X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		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	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X	X	X	X

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Principal	Refer to 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
Inappropriate personal use of the internet / social media / personal email	X	X			X	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		X			X	X	X

Careless use of personal data e.g. holding or transferring data in an insecure manner	X		X			X		
Deliberate actions to breach data protection or network security rules	X	X	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X			X	X	X
Sending an email, text or 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	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	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X
Breaching copyright or licensing regulations	X	X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Policy author / reviewer:	***Policy date / review date:***	***Next review due:***
Ziggi Szafranski	September 2023	September 2024