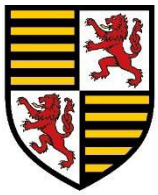


WARMINSTER SCHOOL

E-SAFETY POLICY

Date of Latest Review:	31 August 2023
Responsible Person(s):	Deputy Head, DSL and IT Manager

Introduction

This E-Safety Policy takes account of legislative guidance and sets out the School's approach to online safety. Our aim is to protect and educate the whole School community in their use of technology and have effective mechanisms to identify, intervene and escalate any incident where appropriate.

The School's Governing Body will do 'all that they reasonably can' to limit children's exposure to harmful and inappropriate online material, with appropriate filters and monitoring systems in place, to safeguard staff and pupils.

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

The School will deal with e-safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, such as Safeguarding and Protecting Children Policy and Procedures, Anti-bullying, Child on Child Abuse and Behaviour, Rewards, Sanctions and Discipline. It will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

The School will monitor the impact of this policy using:

- Logs of reported incidents
- Logs of internet activity (including sites visited)
- Internal data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff

Development, Monitoring and Review of this Policy

This E-Safety Policy has been developed by the Deputy Head, DSL and IT Manager and sanctioned by the Senior Leadership Team. Consultation with the whole school community will continually take place through a range of formal and informal meetings.

The implementation of this E-Safety policy will be monitored by the:	Deputy Head, DSL, IT Manager
Monitoring will take place at regular intervals:	At least termly; agenda item on SLT and ET Meetings
The E-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:	31 August 2024
Should serious online safety incidents take place, the following persons / agencies should be informed:	Head, Deputy Head, Designated Safeguarding Lead and Nominated Safeguarding Governors. They will determine the course of action to be taken. If the issue involves safeguarding concerns, then the School's Safeguarding policy will be followed in order to determine whether to inform external persons/agencies

Roles and Responsibilities

The Governing Body

The Governing Body has overall legal responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn. The Governors will ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

The Nominated Governor for Safeguarding and Child Protection takes on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Review meetings with the Designated Safeguarding Lead and Deputy Head
- Monitoring of e-safety incidents in MYCONCERN
- Monitoring of filtering / change control logs
- Reporting to Governing Body as appropriate.

The Head and Leadership Team

The Head has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead.
The Head and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
The Senior Leadership Team will receive regular monitoring reports from the DSL/Deputy Head.

The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for all safeguarding and child protection matters at the School, including online safety, and supports all other staff in dealing with any child protection concerns that arise. The DSL is trained in online safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- **content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
- **contact**: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behavior that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

When necessary, the DSL will liaise with external agencies such as the Multi-Agency Safeguarding Hub (MASH), Early Help or Police.

DSL and Deputy Head

- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provide training, support, and advice for staff
- Along with the Head of PSHE are responsible for e-safety education for pupils
- Liaise with school technical staff
- Monitoring network / internet / incident logs with the IT manager
- Receive, analyse and respond to reports of filtering incidents
- Monitor e-safety incidents in MYCONCERN
- Meet/communicate with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Production, review and monitoring of the school filtering procedures and requests for filtering changes in collaboration with the IT manager
- Report regularly to Senior Leadership Team (in SLT meetings)

IT Manager

The IT Manager is responsible for ensuring that:

- The School's technical infrastructure is secure and is not open to misuse or malicious attack
- The School meets required e-safety technical requirements
- Users may only access the networks and devices through a properly enforced password protection policy, which meets sufficiently high complexity requirements, as well as being checked against known passwords.
- The filtering is applied and updated on a regular basis
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- The use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the Deputy Head for investigation
- Monitoring software and systems are kept up to date.

Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of this e-safety policy and practices
- They have read, understood and agreed to the IT Acceptable Use Policy
- They report any suspected misuse or problem to the Director of E-Learning for investigation
- All digital communications with other staff, pupils and parents are on a professional level
- They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

Pupils

Our pupils:

- Will be involved in the development and review of this Policy through discussion in lessons and other forums, in an age appropriate way.
- Are responsible for using the School ICT systems in accordance with the Pupil Acceptable Use Policy, which is signed when a pupil first joins the School and agreed each year thereafter.
- Will be expected to know and understand policies on the use of Personal devices and cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers their actions out of School, where related to their membership of the School

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents will be invited to attend e-safety training and encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the School (where this is allowed)

Community Users, Visitors and Volunteers

Community Users, visitors and volunteers who require access to School systems are given access to the internet via their own device using a WiFi code/log in (access to school drives/data is restricted) or access to a desktop with the appropriate level of permissions – starting at internet access only.

Policy Statement:

Education – Pupils

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

- A planned e-safety curriculum is provided as part of PSHE and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities. This includes the use of external speakers.
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the Pupil Acceptable Use Policy agreement and encouraged to adopt safe and responsible use both within and outside the School.
- Pupils are helped to understand the benefits associated with social media, online posting and messaging.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT support to remove those sites from the filtered list for those pupils. Any requests to do so should be audited by the IT Manager, and clear reasons for the need must be established and recorded.

Education – Parents and Carers

Parents play an essential role in the education of their children and in the monitoring/regulation of their son or daughter's online behaviour. The School provides information and awareness to parents through seminars, newsletters and the provision of online resources.

Education – Staff and Volunteers

It is essential that all staff who are granted access to the School network receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and overseen by the Director of E-Learning, recorded as having taken place as follows:

- Training is made available to staff and is regularly reinforced. The Deputy Head will ensure that an audit of the E-Safety training needs of all staff with access to the network will be carried out regularly with support of independent trainers when appropriate.
- All new staff are informed of their obligations with regard to E-safety as part of their induction, fully understand and agree to the IT Acceptable Use Policy.
- The Deputy Head and DSL will receive regular updates through attendance at external training.
- This policy and its updates will be presented to and discussed by staff as part of Inset training.
- Updates regarding current online threats will be communicated to all staff (and parents if appropriate).

Education – Governors

The E-Safety Governor will take part in or receive updates of E-Safety training/awareness sessions:

- Attendance at training provided by any relevant organisation
- Monitoring of school training and information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

- 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 technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by IT who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password If the user thinks that their password is known to others, they must inform the IT Support team directly (if they are staff) or a member of teaching staff (if they are a pupil) so that their password can be changed.
- Admin passwords for the various systems are all different. These are all stored in a password manager, (enabling the use of complex and long passwords) which the entire team have access to. If the Head etc needs access, any one of the Support Team can facilitate this. Access to the password manager group can also be granted if required.
- The IT Manager 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's Child Abuse Image Content (CAIC) list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the IT Acceptable Use Agreements.
- The online Help Desk is in place for users to report any actual / potential technical incident / security breach to the relevant person (the IT Manager).
- 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 endpoint protection software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place through the network use policy that forbids staff from downloading executable files and installing programmes on school devices.

Use of digital and video images

Please also see the Staff Code of Conduct. 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 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. 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 e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents 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 comment on any activities involving other pupils in the digital / video images.

- As per the School's Code of Conduct, staff and volunteers should where possible, use School phones, tablets, video, and photography equipment to take images of pupils. School phones and cameras can be borrowed on request. If no school equipment is available, images should be transferred straight onto the school network (using Foldr app) or the individual's School OneDrive and deleted from the personal device and from personal cloud storage areas. All images of children should be stored securely and only accessed by those authorised to do so. Staff should delete any images from their personal media once the picture has been downloaded, posted or stored on the school systems.

When taking photos or videos the following should be considered:

- The purpose of the activity must be clear;
- All images should be open to scrutiny to ensure that they are appropriate;
- Images should not be made during one-to-one situations;
- Ensure that the pupil or pupils are appropriately dressed;
- Ensure that the pupils understand why the picture is being taken;
- Images must not be taken secretively;
- Pupils must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Written permission from parents 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 or parent.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the School considers the following as good practice:

- The official School email service may be regarded as safe and secure. Users should be aware that email communications may be monitored.
- Users must immediately report, to the IT Manager, the HR Manager or their Line Manager (as appropriate) 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 (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging, private messaging apps or social media must not be used for these communications.
- Staff must not contact pupils at home unless absolutely necessary. In such circumstances the School email or Firefly must be used and communication should be restricted to the hours 0730-2130

Social Media – Protecting Professional Identity

The School has a duty of care to provide a safe learning environment for pupils and staff. The School could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, disability (or other protected characteristics) or who defame a third party may render the School liable to the injured party.

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use, social media risks, checking of settings, data protection, reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- 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.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Responding to online safety incidents

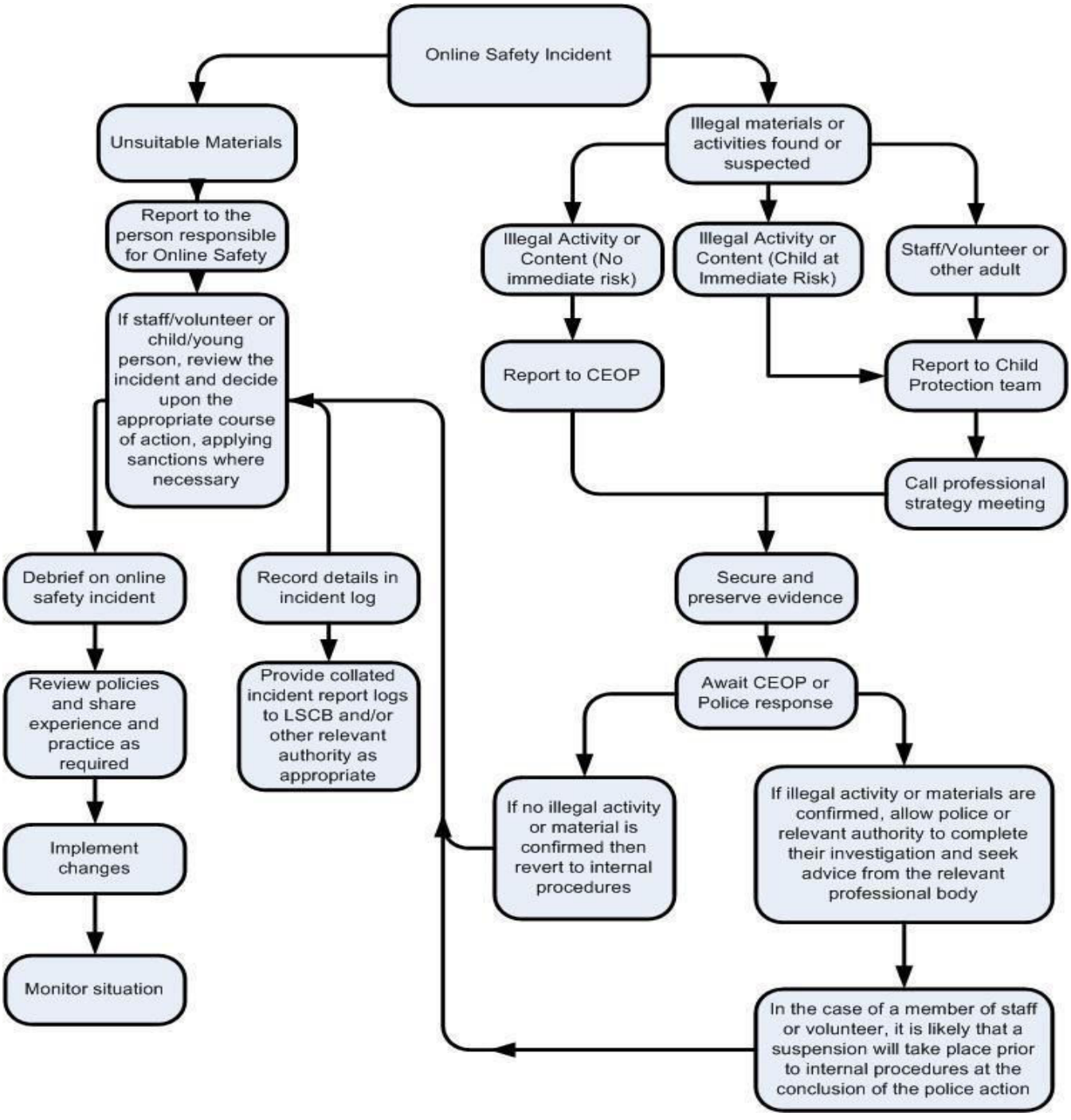
The following guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities; please see Appendix 1 for clarification of

acceptable / unacceptable / illegal online activities. For advice on the production of indecent images (sexting) please refer to the UK Council for Child Internet Safety guidance document, "Sexting in schools and colleges: Responding to incidents and safeguarding young people".

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 A for responding to online safety incidents and report immediately to the police.

Flowchart A – Responding to an online safety incident



Responding to 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 - 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.

Allegations and Sanctions

Safeguarding allegations or concerns about Staff will be handled in accordance with the Safeguarding and Protecting Children Policy and Procedures. Staff misuse of School ICT systems will be dealt with in accordance with the Disciplinary and Dismissal Procedure.

Pupils' misuse of School ICT systems will be dealt with in accordance with the School's Behaviour, Rewards, Discipline and Sanctions Policy

Appendix 1

Acceptable, Unacceptable and illegal uses of ICT

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 (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			
						X

On-line gambling					
On-line shopping / commerce		X			
File sharing				X	
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube					X

V0823