



E-Safety Policy

2026

Reviewed by:	D Towers
Approved by:	Governing Body
Date approved:	March 2026
Review date:	March 2027

Contents

SCOPE AND AIMS OF THE POLICY	3
1. TEACHING AND LEARNING	5
1.1 The importance of Internet Use	5
1.2 Using the Internet to Enhance Learning	5
1.3 Educating Pupils About Online Safety	6
1.4 Remote Learning	8
2. MANAGING INFORMATION SYSTEMS	8
2.1 Maintaining Systems Security	8
2.2 Passwords and Password Security	10
2.3 Email	11
2.4 Published Content	13
2.5 Capture, Generation and Publication Images and Video	13
2.6 Social Networking, Social Media and Personal Publishing	14
2.7 Filtering	16
2.8 Audio and Video Calling	17
2.9 Emerging Technologies and AI	18
2.10 Protection of Personal Data (including confidential data)	19
3. POLICY DECISIONS	21
3.1 How access to the school system/internet will be authorised	21
3.2 Risk Assessment	23
3.3 Responding to Incidents of Concern/Misuse	24
3.4 Handling Online Safety complaints	25
3.5 Online Bullying	26
3.6 Examining Electronic Devices	29
3.7 Microsoft 365 (Teams)	30
3.8 Management of mobile phones and personal devices	31
4. COMMUNICATION POLICY - ONLINE SAFETY	34
4.1 Pupils	34
4.2 Staff	34
4.3 Parental Support	35
5. MAINTENANCE OF SCHOOL ICT SYSTEMS	37
5.1 General	37
5.2 Faults and Damage	37
APPENDICES	39
Online Safety Contacts and References	40
Legal Framework	41

SCOPE AND AIMS OF THE POLICY

The pages which follow set out the Policy for the safe use of Information Communications Technology at St Peter's RC High School. This policy applies to all members of the school (including staff, pupils, volunteers, parents/carers, guests) who have access to and are users of school digital technology 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 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 Safety 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. 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 Safety behaviour that take place out of the school.

In today's society, children, young people and adults interact with technologies such as mobile phones and apps, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

We constantly review our approach on the right balance between controlling access to the Internet and technology, setting rules and boundaries and educating pupils and staff about responsible use. We are also aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Our approach is to empower and educate pupils so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff must be aware of the importance of good Online Safety practice in the classroom in order to educate and protect the children in their care. Members of staff must also be aware of how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

The school has a legal duty to ensure that it has done all in its power to protect users of the system and to keep sensitive data safe and secure. This Online Safety policy is an

honest attempt to cover all the main areas and sets out how we plan to develop and establish our Online Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

It is the responsibility of all Staff to have an up-to-date awareness of online safety matters and understand and follow the procedures outlined in this Online Safety policy. In this way the use of the ICT system at St Peter's will provide a safe learning environment for users, will enhance the curriculum and administration processes, and will ensure that personal and sensitive data is safe and secure.

The school acknowledges the importance of Online Safety both inside and outside the school community. The Headteacher and the school Governors recognise it as an important aspect of strategic leadership within the school and have ultimate responsibility to ensure that the policy and practices relating to Online Safety are embedded and monitored. The school designated lead for Safeguarding is Mrs K Holden (Assistant Headteacher) who will hold overall responsibility for Online Safety.

The Headteacher and Governing body have a legal responsibility to safeguard children and staff, and this includes online activity.

- The school has an appointed DSL Mrs K Holden (Assistant Headteacher) with ultimate responsibility for online safety issues including maintaining a log of online safety issues.
- The e-Safety Policy and its implementation will be reviewed annually.

The Senior Leadership Team and Governing Body will review the Online Safety policy annually and monitor its impact. They will also ensure that they take responsibility for revising the Online Safety policy and practice where necessary (such as after an incident, change in national legislation or the introduction of new technology etc).

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1. Teaching and Learning

1.1 The importance of Internet Use

- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as a useful learning tool and part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

1.2 Using the Internet to Enhance Learning

Developing good practice in Internet use as a tool for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Whilst the Computing curriculum provides pupils with a whole range of digital skills, because of the cross-curricular nature of Internet use, a whole school approach will be adopted.

- The school's Internet access will be designed to enhance and extend education and will include filtering appropriate to the age of the pupils via the school filtering system.

- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. Staff must vet and accept responsibility for the appropriateness of websites they request to add, and follow school procedure:
- Request (sites) to be added via the IT Manager
- Pupils will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use in their Computing curriculum lessons. In addition, all staff will be responsible for reminding pupils of responsible use prior to any Internet session.
- Pupils will be taught the meaning of copyright and to acknowledge the source of information used, in their Computing curriculum lessons. However, all staff should ensure that the use of Internet derived materials used by themselves or pupils comply with copyright law and that sources of information are acknowledged.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. This will be done within the Computing curriculum.

1.3 Educating Pupils About Online Safety

In KS3 and KS4, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once

this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images

- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these

can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their classes/form groups.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

1.4 Remote Learning

In the event of a school closure, the school is committed to providing continuity of education to its learners and will do so through a process of remote (online) learning and other appropriate methods. Extensive remote learning would apply particularly in a situation in which the school is closed for an extended period of time, but a high proportion of learners and teachers are healthy, and able to work as normal from home. This does not normally apply in the event of short-term school closures (e.g. as a result of inclement weather) or a short-term learner absence.

Remote learning may also be appropriate in situations when learners, in agreement with the school, have a period of absence but are able to work at home, at least to some extent. This may apply in cases such as exclusion from school, or longer-term illness, assuming learners are able to complete schoolwork at home. Another relevant instance would be if, following an infectious disease outbreak, learners are self-isolating at home but are not suffering with relevant symptoms.

There is no obligation for the school to provide continuity of education to learners who absent themselves from school, with or without parental permission, in contravention to school or government guidance. This may apply, for example, if parents choose to take learners on holiday during term time. Similarly, this would apply if parents made the decision, without prior agreement with the school, to absent their child from school 'as a precaution', against official guidance, in the event of an outbreak of infectious disease.

A Remote Learning Policy has been developed which will detail procedures for remote home learning.

2. Managing Information Systems

2.1 Maintaining Systems Security

This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue, and this document only touches on relevant areas.

The management of the information systems is the responsibility of the IT Manager and his team. This covers:

Local Area Network (LAN) security issues include:

- Workstations secured against user mistakes and deliberate actions
- Servers and infrastructure devices located securely and physical access restricted
- Server operating systems secured and kept up to date
- Virus protection for the whole network kept up to date and current

Wide Area Network (WAN) security issues include:

- Decisions on WAN security are made in partnership with the school management team.
- The responsibility for protecting the school's broadband network lies with the IT Manager in partnership with the school management team.
- The security of the school information systems and users will be reviewed regularly by the IT Manager and school management team.
- Backing up of the system, configuration of the school's internet firewall and web filtering, and updating of the anti-virus system are the responsibility of the IT Manager.
- The security of the school's ICT systems will be periodically audited by independent external contractors

All Users:

- There are different access levels for different user groups e.g. Technicians, Administrators, Leadership, Staff and Pupils.
- Portable media may only be used following the school procedure. Where staff have been given specific permission from the Headteacher to use portable media, they will be responsible for virus/malware checks and maintaining the security of the data contained on the portable media.
- Unapproved software will not be allowed to be stored in work areas or attached to email or uploaded via one drive or Teams.
- All users must act reasonably. Users must not access other people's files without express permission from the Headteacher and then only in the presence of a member of the Leadership Team. They should not corrupt, interfere with or destroy any other user's information.
- Loading (downloading or uploading) of software is not allowed by users. The installation of software can only be carried out by IT technical support staff.

- The use of user logins and passwords to access the school network will be enforced.
- All users should logout after use. Failure of all users (pupils and staff) to logout after use or to keep passwords secure can compromise the security of the whole network.
- Under no circumstances should any user log on to the system using a login and password which is not their own. This constitutes an extremely serious offence, and disciplinary action may be taken for staff/adults flouting this rule.
- Pupils who allow their passwords to be used by others will lose their network privilege as will the offending pupils and school disciplinary action will follow.
- It is a disciplinary offence for staff to allow their user id and password to be used by others.
- The downloading of large files such as mp4's can compromise the system performance and should only be carried out by ICT Technical Support staff technicians.
- Users (other than named staff) will not have access to portable storage. Pupils studying photography are exempt from this and have a designated space on the school network where different rules apply.
- All portable storage devices e.g. Flash Memory Sticks must be given to the ICT Technical Support Staff who will be responsible for reading and writing data, checking the suitability of the files and virus checking before transferring any data onto the school network. Pupils must obtain permission from their teachers before using transferable media for coursework and homework. Users will be notified of the times when this service will be available. Pupils may be asked for proof of identity.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas (including cloud storage areas) or attached to email.
- Although the Filtering system is robust, it is not fool proof. Use of the school network/Internet to attempt to access or access inappropriate materials such as pornographic, racist, radical or offensive material is forbidden. All sites visited are logged and will also leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

2.2 Passwords and Password Security

Password security is essential for staff, particularly as they are able to access and process pupil data. All users are expected to have secure passwords which are not shared with anyone. Staff and pupils are regularly reminded of the need for password security. The school considers the following to be good practice:

- Always use your own personal passwords and never attempt to logon with another user's user id and password.
- Any temporary passwords should be changed at first logon
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised IT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Staff must never reveal their password to a pupil or colleague
- If you aware of a breach of security with your password or account inform the IT Manager immediately
- If you think your password may have been compromised or someone else has become aware of your password report this to the IT support team and change your password

Passwords should be changed every six months. They must contain a minimum of eight characters and be difficult to guess. They should also contain a mixture of upper and lowercase letters, numbers and symbols.

User ID and passwords for staff and pupils who have left the school are removed from the system on the date they leave or as soon thereafter.

The 'master/administrator' passwords for the school used by the technical support staff must also be available to the Headteacher and kept in a secure place e.g. school safe.

2.3 Email

It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

All pupils have a school email address. Presently, they are only able to receive emails from members of staff and selected software providers e.g. Sparks. However, there may be occasions when pupils are allowed to send emails when doing specific school projects for example. In such cases pupils must follow the guidance in the ICT Responsible Use Agreement. Email addresses do not identify a pupil's full name.

Spam, phishing and virus attachments can make email dangerous. The preferred filtering system is designed to stop unsuitable email getting through.

Access, on school equipment, to most external personal email accounts is blocked. All email should be written carefully and politely. Offensive or abusive language in messages or any language which could be considered defamatory, obscene, menacing or illegal must not be used nor should language that could be calculated to incite hatred against any ethnic, religious or other minority. As messages may be forwarded, email is best regarded as public property.

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 can be monitored.
- Staff will only use official school provided email accounts for educational/business purposes. The use of personal email accounts during school hours on school equipment is not allowed neither is the use of personal email accounts for school purposes at any time.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, personal text messaging or personal social media accounts must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Pupils may only use approved email accounts for specific school purposes as requested by members of staff.
- Pupil email sent to any external organisation should be authorised by a member of staff and written carefully before sending, in the same way as a letter written on school headed paper. Such email should be checked by the teacher before sending.
- Pupils must immediately tell a member of staff if they receive an email/message that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. The member of staff must pass this on to the DSL. Other users receiving offensive email, including offensive spam, should inform the IT Network Manager and the DSL.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Pupils must not reveal personal details of themselves or others in email/message communication, or arrange to meet anyone without specific permission from an adult.
- Personal details including phone numbers, or personal e-mail addresses of any colleague or pupil must not be given over the Internet.

2.4 Published Content

School websites provide opportunities to celebrate pupils' work promote the school and publish resources for projects.

Publication of any information online should always be considered from a personal and school security viewpoint.

- The contact details on the school website will be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Faculty/Department Heads will be responsible for ensuring that content relating to their subject areas is accurate, appropriate and up to date. They will also be responsible for approving any links to other Internet sites.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with statutory obligations and with the school's guidelines for publications including respect for intellectual property rights, policies and copyright.

2.5 Capture, Generation and Publication Images and Video

Digital images are easy to capture, reproduce and publish and, therefore, open to misuse. It is not appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. The security of staff and pupils is paramount.

Recording Images/Videos

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images/videos of pupils, this includes when on field trips. There may be an exceptional circumstance where the Headteacher may give permission for this rule to be waived. In such circumstances staff must obtain written permission. Images/videos must be transferred as soon as possible and solely to the school's network or cloud account and deleted from any staff personal device. Images/videos of pupils must not be stored on personal digital devices.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images/videos/sound of pupils, staff and others without advance permission from the Headteacher
- In all cases images/videos/sound must not be taken without the consent of the person/people whose image is being taken.
- All staff and pupils must not under any circumstances make use of generative AI to create images, sounds or video depicting or mimicking any member of the school community without express permission from

the Headteacher and the subject of the image. When seeking permission, a clear and appropriate reason must be stated.

Publication of Images

- Images or videos that include pupils should be selected carefully and parents/carers permission will be obtained before being electronically published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs without the express permission of parents/carers.
- Pupils' work can only be published with their permission or that of the parents/carers.
- A record of consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- Images obtained without the required consent/permission must not be published on any digital media including social media.

2.6 Social Networking, Social Media and Personal Publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites provide on-line communities and can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, social networking, forums, multiplayer online gaming, chatrooms, instant messenger, snapchat, twitter, Instagram, tik tok and many others.

- Access to social media and social networking sites will be controlled in school by the use of the Internet filtering system.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use personal social media to infringe on the rights and privacy of others or to make ill-

considered comments or judgements about the school, its pupils, parents/carers, staff or any member of the school community.

- Staff must ensure that confidentiality in relation to members of the school community is maintained on social media even after they leave the employment of the school.
- Pupils will be advised, during their Computing curriculum lessons and special assemblies, never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. They will also be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be taught and encouraged, through the Computing curriculum, how to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Staff wishing to create a Social Media account to support their work with pupils as part of the curriculum must present a business case to the School Leadership Team who will approve or reject it as appropriate. Staff must obtain documented consent from the SLT before using Social Media tools in the classroom.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups and chatrooms will be blocked unless a specific use is approved.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly pupils use of sites with an age restriction.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school ICT Systems Code of Practice and Agreement, together with the potential consequences of unacceptable online behaviour both professional and personal.
- Pupil personal use of social networking, social media and personal publishing sites will be discussed as part of the Computing Online Safety module.
- The consequence of unacceptable online behaviour for pupils is outlined in the ICT Responsible Use and BYOD Agreement/Codes of practice for pupils.

Process for creating new school social media accounts

The school community is encouraged to consider if a social media account will help them in their work e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:

- The aim of the account

- The intended audience
- How the account will be promoted
- Who will run the account (at least two members of staff should be named)
- Will the account be open or private/closed.

Following consideration by the SLT an application will be approved or rejected. In all cases the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training.

2.7 Filtering

The management of Internet filtering lies with the IT Manager. The filtering system uses categories of allowed sites and blocked sites, which are updated regularly by the filtering provider. These categories can be overridden, by school IT staff upon request, to block or allow access to particular sites within a category.

Access profiles will be appropriate for all members of the school community. As part of a supervised project, pupils might need to access specific adult materials; for instance, a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. It may be possible to temporarily change the access profile to the pupil's age and maturity subject to prior notice being given and a risk assessment undertaken.

It is important that we recognise that filtering is not 100% effective. Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems.

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that pupils should always be supervised when using Internet access.

In addition, Internet Safety Rules should be displayed, and both pupils and adults should be aware of the risks online. An incident Log to report breaches of filtering or inappropriate content being accessed will be maintained and procedures for reporting to parents will be followed as appropriate.

Teachers should always evaluate any websites before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The Internet filtering policy will be under continual review.
- The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be made aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL must be reported to the school DSL and the IT Manager who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team. Any material that the school believes is illegal will be reported to appropriate agencies such as the Police or CEOP.

2.8 Audio and Video Calling

The school's access strategy will be designed to suit the age and curriculum requirements of the pupils, with advice from the IT Manager and Senior Leadership Team as appropriate.

Video Conferencing e.g. Teams, Zoom, Google Meet:

- Conferences should always be booked as private and not made public.
- The contact details for example Skype name, URL, should only be given to those who you wish to take part.
- Check who has signed into your conference as it is possible for a guest without a camera not to be visible.
- Wherever possible, staff must make use of the "lobby" feature of online meeting systems to ensure that only the desired attendees of the meeting are granted access.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information will not be put on the school website.
- The equipment (e.g. web cams) will be kept secure and if necessary locked away when not in use.
- Responsibility for the use of the videoconferencing outside school time will be established with care.

Users

- Pupils will not have access to initiate or make conference calls.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote-control pages.

- Usernames and passwords for video conferencing e.g. Zoom, should only be issued to members of staff and kept secure.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given, and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third-party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non- school site, it is important to check that they are delivering material that is appropriate for your class.

An additional point to consider is that participants in 3rd party organisations may not be DBS (previously CRB) checked.

2.9 Emerging Technologies and AI

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications. Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within the school system. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

St Peter's recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St Peter's will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and

should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

School leadership and staff will endeavour to keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. We already use the EduLink to digitally communicate with parents/carers.

- Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.
- Staff and pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Computer/Internet Use Code of Practice.
- Staff **personal** mobile devices must not be used to communicate with pupils or families, unless authorised in writing by the Headteacher.
- Pupils will be reminded that the use of inappropriate/abusive language or images when communicating with others via mobile technology in and out of school is unacceptable and can lead to serious consequences.
- The taking, storage or sending of photographs, videos or sound recordings without the consent of those involved is not allowed.
- The school policy relating to mobile phones will be followed. The use of personal mobile devices (including 'phones) by staff and pupils is not permitted during lessons or formal school time, unless such devices are being used as part of the lesson and for educational purposes using the school Wi-Fi network and in accordance with the BYOD policy. In addition, uploading to the school system via the use of any new emerging technologies is only allowed by the IT Support Team.
- YouTube will only be accessible by teaching staff and other designated staff, in order to allow them to filter resources which are suitable for classroom use. Teachers will take full responsibility for YouTube resources they show in classrooms and in all cases must always check with Subject Leaders/Faculty Heads as to appropriateness for age and suitability. Teachers will be responsible for ensuring that inappropriate images e.g. in advertisements are not displayed. This will require careful planning and the video being displayed on full screen ready for classroom use. Under no circumstances must pupils be allowed to access YouTube. Should there be any doubt about the appropriateness of resources Subject Leaders/Faculty Heads must seek the advice from the DSL.

2.10 Protection of Personal Data (including confidential data)

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

This section of the Policy is a reminder that all data from which people can be identified must, by law, be protected.

The Data Protection Act 2018 alongside the GDPR applies to anyone who handles or has access to information concerning individuals. **Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.** Please refer to the School Data Protection Policy.

Data Security

It is essential that the privacy of all personal data is maintained. All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on removable storage media, that media must itself be password protected, kept in a locked filing cabinet, drawer, or safe.

Data breaches can have serious effects on individuals and /or the school community, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the School Data Protection Policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

In order to maintain the privacy of personal data:

- Users may not remove or copy sensitive or restricted or protected personal data from the school without permission and unless the media is encrypted or password protected.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when being used off the school premises.
- When restricted or protected personal data is required by an authorised user from outside the school premises (e.g. a member of staff working from their own home) they should use the school's remote access

systems (EduLink).

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software/passwords. They should also ensure they are adequately protected and secured.

Breaches of Data Security

The school has a duty to take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. The ICO (Information Commissioner's Office) Guidance on Data Security Breach Management will be referred to and followed, as appropriate, in such events.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment (both personal and school) on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Human Error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Blagging offences where information is obtained by deceiving the organisation who holds it

Any data security breach or suspected breach must be reported to the Headteacher immediately. The Headteacher will assess the risk and will refer to and follow the Breach

Management Plan below as appropriate.:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

3. Policy Decisions

3.1 How access to the school system/internet will be authorised

The school allocates Internet access to staff and pupils on the basis of educational need. It is made clear who has Internet access and who has not. Authorisation is on an individual basis.

All pupils, staff and guest users (at the school's discretion) will have access to the school network and Internet via their official user accounts. Access, including Internet access is granted on the basis that all users will act responsibly in accordance with the Computer/Internet Use Code of Practice and BYOD Code of Practice.

Guests/visitors using their own devices/content with pupils and staff must be made aware that all materials to be presented should be suitable and age-appropriate for the intended audience and in accordance with the ICT Responsible Use/BYOD Agreement. The member of school staff responsible for the guest/visitor must remain in the room when these materials are being presented.

Parental/carer permission is requested for Internet/Network access by pupils. A record of parental consent is maintained. Pupils are not prevented from accessing the Internet unless the parents/carers have specifically denied permission or the pupil is subject to a sanction as part of the school Computer/Internet Use Code of Practice.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff are required to agree to the terms set out in the 'Staff computer/Internet Use Code of Conduct' before using any school ICT resources. This will be completed at the start of each Academic Year or, in the case of new employees, from the date of their commencement.
- All visitors to the school site who require access to the school's network or Internet access will be asked to agree to the terms of the 'Computer/Internet Use and BYOD Code of Conduct'.
- When considering access for vulnerable members of the school community (such as children with special educational needs) the school will make decisions based on the specific needs and understanding of the pupil(s) in consultation with the Inclusion Faculty.
- Pupils will apply online for Internet/Network access individually by agreeing to comply with the 'Responsible Use Code of Practice and BYOD Agreement Form'.
- Parents/Carers will be asked to read and discuss the 'Responsible Use Code of Practice and BYOD Agreement Form' with their child. They will be asked to agree to the terms of the Agreement by completing an online Form.
- There will be an interim period of one week (2 weeks for pupils) when restricted access to the ICT system will be permitted. This will give users ample opportunity to complete the online agreement form.
- Appropriate staff will be notified if a pupil has been denied access to the Internet for inappropriate use.
- All users will be made aware of the consequences of unacceptable use, and these will be clearly stated in the 'Computer/Internet Use and BYOD Code of Practice'
- The school reserves the right to withdraw the access of any user who violates the

'Computer/Internet Use and BYOD Code of Conduct'. (A copy of the 'Computer/Internet Use and BYOD Code of Practice' for Staff and Pupils can be found in the appendix.)

3.2 Risk Assessment

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

Risks can be considerably greater where tools are used which are beyond the school's control such as most popular social media sites.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to relevant authorities.
- A risk assessment will be carried out before the introduction of any new technology.
- Methods to identify, assess and minimise risks will be reviewed regularly.

3.3 Responding to Incidents of Concern/Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

We recognise and seek to develop the skills that pupils need when communicating and using technologies enabling them to keep safe and secure and act with respect for others.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of the school ICT systems, the level of response necessary will be determined for the offence disclosed e.g. involving the police.

Staff Incidents

- If any member of staff is suspected of engaging in inappropriate or illegal Online activity this must be reported immediately to the Headteacher and the Deputy Headteacher responsible for Safeguarding (DSL). The matter will be investigated and appropriate action taken, including informing the necessary authorities as appropriate.
- If any member of staff is the subject of online bullying or receives any inappropriate messages or images or is aware of misrepresentation on social media, this should be reported immediately to the Headteacher and the Deputy Headteacher responsible for Safeguarding (DSL).
- Online activity may be monitored by the IT Manager with permission from the Headteacher and in the presence of a member of the SLT.

Pupil Incidents

- Any Online misuse by pupils must be reported using the Online Safety Reporting Form. A copy of this is automatically forwarded to the IT Manager and the DSL who will escalate the incident accordingly.
- All reported incidents will be recorded and actions taken in the school Online Safety incident log and in any other relevant areas e.g. SIMS.
- The Designated Lead for Safeguarding must be informed of any Online Safety incidents involving child protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- Internet Activity will be monitored daily and a weekly report made.

Incidents of concern will be recorded and raised with the appropriate staff and action taken as necessary.

- The school will inform parents/carers of any incidents of concern as and when appropriate.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place the school will contact the relevant authorities and escalate the concern to the Police.

If an incident of concern relating to child protection needs to be passed beyond the school, then the school DSL will escalate the concern to the appropriate authorities.

3.4 Handling Online Safety complaints

Prompt action will be taken if a complaint regarding irresponsible use is made. The facts of the incident or concern will be established and evidence gathered where possible and appropriate. Online Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious, and a range of sanctions may then be required. Potential child protection or illegal issues must be referred to the school DSL and Online Safety Coordinator.

Complaints

Prompt action will be required if a complaint regarding irresponsible use is made. The facts of the case will need to be established, for instance time, people involved etc.

Pupils

- Complaints about irresponsible use must be reported, using the Online reporting form, Guardian or in person to a member of staff.
- Pupils and parents/carers will be informed of the complaints procedure.
- All Online safety complaints and incidents will be dealt with and recorded by the school, including any actions taken.
- Parents/Carers and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community should be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's

behaviour and child protection procedures.

- All members of the school community will be reminded about safe and appropriate behaviour online (in and out of school) and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- There may be occasions when the police must be contacted. This is a decision the Headteacher/DSL/Online Safety Coordinator will make when all the facts are presented.

Sanctions available include:

- Normal classroom discipline procedures.
- Interview and/or counselling by Head of Computing, Head of Year, Deputy Headteacher, Headteacher, as appropriate.
- Informing parents/carers.
- Removal of computer and/or Internet access for a period which could prevent access to schoolwork held on the system including examination coursework.
- Interview with parents/carers if deemed appropriate.
- Invoicing parents/carers as necessary.
- Informing outside Agencies as necessary.
- Suspension and in some cases exclusion for serious breaches.

Staff

Any complaint about staff misuse must be referred to the Headteacher.

Sanctions available include:

- Interview with Line Manager, Deputy Headteacher, Headteacher
- Disciplinary action up to and including dismissal

3.5 Online Bullying

Online or Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. This can include harassment, threatening or intimidating someone, and encompasses all forms of online bullying including, for example, sexting and racist slurs.

Many young people and adults find that using the Internet, mobile phones and other mobile media, is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via

mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand online bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how online bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted upon.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If the school feels that an offence may have been committed, advice from the police will be sought.

Online bullying on or off site (along with all other forms of bullying) of any member of the school community will not be tolerated. The school has a comprehensive anti- bullying policy.

Pupils can report online bullying through the 'guardian system' or to a member of staff. The DSL must be informed of any reported cyberbullying so that incidents can be recorded and appropriate procedures followed.

All incidents of online bullying reported to the school will be recorded.

There are clear procedures in place to investigate incidents or allegations of online bullying, and to support anyone in the school community affected by online bullying:

- Pupils, staff, and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, and appropriate action taken. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff, and parents/carers will be required to collaborate with the school to support the approach to online bullying and the school's Online Safety ethos.
- Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.

Sanctions for those involved in online bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the school's anti-bullying, behaviour policy, or Computer/Internet Use Code of Practice.
- Parent/carers of pupils will be informed.
- If a criminal offence is suspected, The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable. They will also work with external services if it is deemed necessary to do so.

3.6 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be conducted, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from [the headteacher / DSL / appropriate staff member]
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

3.7 Microsoft 365 (Teams)

Office 365 (Teams) is the preferred software for online learning and communication between pupils and staff both in school and remotely (including homework)

Microsoft accounts including belong to St Peter's RC High School. Teams is a professional platform for pupils and staff to use to support learning at home (including homework) and in school. It is our preferred software for online learning and learning related communication between pupils and staff.

The guidance given to staff in the addendum to the ICT Responsible Use Agreement for staff for Remote Learning will apply when using TEAMS at all other times. The guidance for pupils is clearly set out in the ICT Responsible Use Agreement for pupils.

Failure to follow this guidance for both staff and pupils can result in the same sanctions outlined in section 3.4 of this document.

- Pupils/staff will be advised about acceptable conduct and use when using the Teams and the 'Computer/Internet Code of Practice' applies.
- Only members of the current pupil, parent/carers and staff community will have access to Teams.
- All users will be mindful of copyright issues and will only upload appropriate content to Teams.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.
- Any concerns about content placed on Microsoft 365 should be reported in the first instance to the IT Network Manager who will escalate as appropriate. Concerns will be dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or

- offensive.
- The material will be removed by the IT Network Manager if the user does not comply.
- Access to Microsoft 365 for the user may be suspended.
- SLT will be informed.
- All staff must be aware of the importance of data security when using Microsoft 365, including Teams, as outlined in Section 2.10 of this document and the importance of safeguarding when live streaming lessons

3.8 Management of mobile phones and personal devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs etc. are an everyday item in today's society. Mobile phones and other Internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and Internet access all common features. However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their misuse can render pupils or staff subject to cyberbullying.
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

Due to the widespread use of personal devices, it is essential that we take steps to ensure mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms. Staff will be given clear boundaries on professional use.

- The use of mobile phones and other personal devices by pupils and staff in school is covered by the school rules and the 'Computer/Internet Use and BYOD Code of Practice.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices by any member of the school community is forbidden and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or anti-bullying policy as described in section 3.6 of this document.
- Mobile phones and personal devices are not to be used during lessons unless the teacher has given permission as part of the lesson and then only through the school Wi-Fi system following the BYOD policy, nor should they be used in formal school time e.g. assemblies. They should be switched to

'silent' or 'off' mode during these times.

- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site i.e. changing rooms and toilets.

Pupil Use of Personal Devices

- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers in an emergency, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices, and they will be made aware of boundaries and consequences.
- Devices loaned to pupils are essentially to support schoolwork. They are subject to the Device/Laptop Agreement signed by the pupil and parent/carer.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting pupils and their families within or outside of the school in a professional capacity.
- In an emergency e.g. on a school trip, where contact with pupils or parents/carers is or may be required permission may be sought from the Headteacher to use staff personal mobile phones.
- Mobile phones and devices must be switched to 'silent' or 'off' mode during lesson time, unless they are being used as part of the lesson for educational purposes and their use is within the remit of the BYOD policy. Bluetooth communication should be "hidden" or switched off and mobile.
- If members of staff have an educational reason to allow pupils to use mobile phones or personal devices as part of an educational activity, then it must be through the school Wi-Fi network and within the remit of the BYOD policy.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff should not use their own personal devices e.g. laptop, tablet, i-pad to deliver lessons or work with pupils, as the school cannot be responsible for the content accessed on such devices. This does not apply to devices mentioned in the BYOD policy where the school Wi-Fi network is used.

- Devices loaned to staff by the school e.g. laptops or i-pads which are accessed outside of the school network are essentially to support professional activity. These devices are not intended for third party use and members of staff must be aware that they are responsible for the maintenance of confidentiality of school information that may be held on such devices.
- Laptops and other devices loaned to staff are subject to the Laptop/Device Agreement signed by the member of staff.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

4. Communication Policy - Online Safety

4.1 Pupils

Online Safety will be introduced and discussed with pupils through the Computing curriculum. Posters displaying Online Safety rules are available for display in every classroom. The importance of Online Safety will be reinforced through a programme of Year Assemblies and cross-curricular Online Safety week. Reminders about responsible and safe use should precede lessons where computers and the Internet are being used.

- All users will be informed that network and Internet use will be monitored.
- An Online safety training programme for staff will be established to raise the awareness and importance of safe and responsible Internet use amongst pupils.
- An Online safety module will be included in the PSHE, Citizenship and/or Computing programmes covering both safe school and home use.
- Online Safety rules will be posted in classrooms that have Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

4.2 Staff

This school Online Safety Policy will only be effective if all staff subscribe to its values and methods.

All staff must understand that the rules for information systems misuse are specific and that instances resulting in disciplinary procedures and dismissal have occurred.

If a member of staff is concerned about any aspect of their ICT or Internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Induction of new staff includes a discussion about the school Online Safety Policy.

- New staff will be made aware of The Online Safety Policy and where it can be found.
- To protect all staff and pupils, the school will implement a Code of Practice which all users must agree to and sign.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Ongoing and up-to-date appropriate staff training in Online Safety, both professionally and personally, will be available for all members of staff as required.
- Staff nominated to monitor ICT use will be supervised by the IT Manager and will have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their professional role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The school has invested in the training of A CEOP ambassador who will provide training for staff and pupils.

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 can be monitored.
- Users must immediately report to the nominated person (teacher for pupils, DSL for staff) any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication (e.g. email, Teams, digital marking of work etc) between staff and pupils or parents/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.

4.3 Parental Support

Internet use in pupils' homes is increasing rapidly, encouraged by low-cost access and

developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. Parents will be advised of the importance of Online Safety and of suitably helpful organisations.

Parents' attention will be drawn to Online Safety in newsletters and on the school website.

- A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use,
- Parents/Carers will be requested to sign an Online safety/Internet agreement.
- Parents will be encouraged to read the school Code of Practice for pupils and discuss its implications with their children.
- Information and guidance for parents on Online safety will be made available on the school website
- Interested parents can contact the school if they require further help and support.

5. Maintenance of School ICT Systems

5.1 General

Computer equipment must be respected if it is to last and, responsibility for this rests with those in charge and the people who use it. Systems need to be maintained regularly, and repairs/problems dealt with promptly. Early notification of damage/problems is essential if the system is to be maintained efficiently. If problems are not reported, they cannot be dealt with. For problems relating to hardware and software staff must first log a call with IT technical support team. Responsibility for the maintenance of the system lies with the IT Manager.

- The IT Manager and the technical support team will be responsible for maintaining the servers and hardware in order to maintain the efficient upkeep of the system. This will include setting appropriate network space for all users.
- All purchases of hardware must go through the IT Manager who will advise on suitability for system compatibility and supplier.
- All purchases of software must go through the IT Manager who will advise on system compatibility, licensing and supplier.
- All hardware and software will be installed by the IT technical support team. Items purchased without the approval of the IT Manager will not be installed.
- An assets register of all hardware, software and licenses will be maintained and updated yearly by IT Manager.

5.2 Faults and Damage

It is the responsibility of the classroom teacher/supervisor to ensure that ICT equipment is used in a responsible and appropriate manner by the pupils. Computers must be shut down at the end day, and all projectors must be switched off.

- Classroom teachers should regularly remind pupils that they will be held responsible for damage to equipment through irresponsible behaviour.
- Staff should report any pupil found deliberately damaging computer equipment to the IT Manager.
- Parents/Carers of pupils who deliberately damage ICT equipment will be informed and invoiced.
- The cost of wear and tear problems with ICT equipment will be the responsibility of the school e.g. hard drive failure, projector bulbs. ALL other costs for damage caused through irresponsible behaviour of pupils e.g. deliberate damage to keyboard, mouse etc, will be the responsibility of the curriculum area of the

- teacher present in the classroom when and where the damage occurred.
- Faults should be logged with the IT technical support team. Under no circumstances should staff or pupils attempt to repair a fault, tamper with cables or move any equipment i.e. computers, monitors, printers, keyboards, mice etc
 - Staff dissatisfied with maintenance procedures or quality of service should see the IT Manager in the first instance, who has overall responsibility for ensuring that the system is meeting the needs of colleagues.
 - If a data loss or security breach occurs, the Headteacher must be notified immediately, and appropriate action will be taken (see section 2.9).

ACKNOWLEDGEMENTS: *The school thanks Kent County Council for permission to use their Online Safety Policy template.*

APPENDICES

Appendix 1: Online Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Internet Watch Foundation (IWF): www.iwf.org.uk

Teach Today: <http://www.teachtoday.de/en/>

Think U Know website: www.thinkuknow.co.uk

Information Commissioner's Office – Data Protection: www.ico.gov.uk/

Appendix 2: Legal Framework

Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the Internet.

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison. The offence of

grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Schools should have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent, there is no need to prove any intent or purpose.

Data Protection Act 2018 and GDPR

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files).
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission. The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of

communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network.

Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image” 63 (6) must be “grossly offensive, disgusting or otherwise obscene” 63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is

threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.