ST PETER'S

PREPARATORY SCHOOL

Online Safety Policy

Updated on 29 April 2025
by Mr Dan Morris
(Director of Operations & Compliance)

Approved by Head: Charlotte P Johnston.

Date: 07 May 2025

Introduction

It is the duty of St Peter's Preparatory School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles;
- Mobile internet devices such as smartphones and tablets and
- Smart watches and other activity tracking devices.

This policy, in conjunction with the IT use policy for all staff, visitors and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies and guidance documents found in the staff handbook:

- Child Protection and Safeguarding Policy
- Staff Behaviour (Staff Handbook)
- Health and Safety Policy;
- Behaviour, Discipline and Exclusion Policy;
- Anti-Bullying Policy;
- IT Acceptable Use Policy;
- Data Protection Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Peter's Preparatory School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas. Details on how this is carried out can be found in the Curriculum Policy statement and its associated documentation.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the IT use policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, activity trackers and media players etc.).

This policy also supports the School's compliance with the **Protect Duty (Martyn's Law)**, recognising that online environments may contribute to risks of radicalisation and terrorism, which the School mitigates through online safety education and safeguarding processes.

Roles and responsibilities

1. The Head and Senior Management

The Head and Senior management of the school are responsible for the approval of this policy and for reviewing its effectiveness. A designated senior manager will review this policy at least annually.

2. Designated Safeguarding Lead and/or Director of Operations & Compliance

The Head is also responsible for the safety of the members of the School community and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the Deputy Head, Pastoral and the Director of Operations & Compliance. They should ensure that:

- Staff are adequately trained about e-safety;
- Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

- This policy is upheld by all members of the school community, and work with staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

3. IT staff

The outsourced IT management company, CAPtech, has a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for training the School's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Director of Operations & Compliance and Deputy Head, Pastoral.

4. Teaching and support staff

All staff are required to sign the IT use policy before accessing the School's systems.

As with all issues of safety at this School, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Guidance may be sought from the Computing and PSHEE Curriculum leaders in addition to the Deputy Head, Pastoral, CAPtech and Director of Operations & Compliance.

5. Pupils

Pupils are responsible for using the School IT systems in accordance with the Pupil IT use policy, and for letting staff know if they see IT systems being misused.

6. Parents and carers

St Peter's Preparatory School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of School. We regularly consult and discuss e-safety with parents through workshops and documentation, and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

Parents and carers are responsible for endorsing the School's pupil IT use policy.

Education and training

1. Staff: awareness and training

New staff receive information on St Peter's e-Safety and IT use policies as part of their induction.

All staff receive regular information and training on e-safety issues in the form of termly Safeguarding INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff and contractors receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School e-Safety procedures. These behaviours are summarised in the IT use policy which must be signed and returned before use of technologies in School. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines. They re-sign the document at the start of each academic year.

Staff will also be made aware of emerging risks related to artificial intelligence (AI) technologies, including deep fakes, online misinformation, and AI-assisted grooming techniques, and how to address these risks with pupils sensitively and proactively.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the Deputy Head, Pastoral and/or Director of Operations & Compliance.

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about e-safety within a range of curriculum areas and Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside School will also be carried out via PSHEE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, usually via PSHE, pupils are taught about their e-safety responsibilities and to look after their own online safety. From year 6 pupils are informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Deputy Head, Pastoral, Designated Safeguarding Leads and/or any member of staff at the school.

From year 3, pupils are also gradually taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities. Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers

cases of bullying). Pupils should approach any member of staff as well as parents, or peers for advice or help if they experience problems when using the internet and related technologies.

3. Parents

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and guardians may feel equipped to protect their child(ren) when they use electronic equipment at home. The School therefore arranges regular workshop discussion opportunities for parents offering guidance about e-safety and the practical steps that parents can take to minimise the potential dangers to their child(ren)] without curbing their natural enthusiasm and curiosity.

Policy Statements

1. Use of School and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at St Peter's are permitted to bring in personal devices. However, staff are not allowed to have their personal devices switched on during the working day, unless they are being used for work purposes. All personal devices brought into School who wish to connect

to the school network should be authorised by the DIrector of Operations & Compliance, who instruct the IT Support Officer to provide the necessary security settings to access the school wifi network and internet filtering protocols. Without these the device will not function correctly.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system unless the device has been sanctioned for such use.

Pupils

Boarders must hand all personal portable devices to the Boarding parents during the school day.

If pupils bring in mobile devices, they should be kept switched off and handed to the main receptionist for the duration of the school day and collected at de-registration. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The School allows the use of pupil owned Chromebooks as a teaching and learning tool for pupils with a designated SEND. These pupils are required to have their devices authorised by the IT Support Officer and/or management company, CAPtech,, who should provide the necessary security settings to access the school wifi network and internet filtering protocols. Without these, the device will not function correctly. They should also adhere to the pupil IT use policy which prohibits pupils from using tablets for non-school related activities during the school day. The Head of Learning Success will inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at School.

School mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored in various charging stations across the school site. Access is available via teaching staff. Laptops and iPads should be signed out and in before and after each use by a pupil. Chromebooks are supervised by the teaching staff where the devices are kept.

2. Use of internet, social media and email

Staff

Staff must not access social networking sites, personal email or any website or personal email which is unconnected with school work or business from school devices or whilst teaching. Such access is restricted by the School's IT security systems but, when available, should only be made from staff members' own devices whilst in the staff room.

When accessing social networking sites out of School hours, staff should do so with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school. They should adhere to the school's Social Media Policy as found in the staff handbook.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the School network and staff email addresses are monitored.

Staff must immediately report to the Head, via Director of Operations & Compliance, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Director of Operations & Compliance, IT Support Officer and/or IT management company, CAPtech.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring St Peter's Preparatory School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;-using social media to bully another individual;
- posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or ex pupils be added as social network 'friends' or contacted through social media. Staff should be mindful of having parents as social network "friends" and are asked to exercise discretion and caution when doing so.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or

parent / carer using any personal email address. The School ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school assignments, research and projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work purposes, pupils should tell a member of staff who will contact the IT Support Officer, in the first instance, for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to a member of staff.

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to a member of staff who will advise the IT Support Officer, DSL and Director of Operations & Compliance. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the IT Support Officer, in the first instance, for assistance.

3. Data storage and processing

The school takes its compliance with the General Data Protection Regulation 2018 seriously. The Retention of Records and Information Security policy outlines the school's policy on data management.

Staff and pupils are expected to save all data relating to their work in their School Google Drive account.

Staff devices should be encrypted if any School data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on removable media.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head.

4. Password security

Pupils and staff have individual school network logins, email addresses, and access to shared storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

- All pupils and members of staff should:
- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every [6] months;
- not write passwords down; and
- not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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

Parents / carers or other family members are permitted to take digital video and images of their own children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published anywhere online; blogs or social networking sites.

Staff and permitted volunteers are allowed to take digital / video images to support educational aims, but must follow this policy, and the use of digital imagery policy with

regards to the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others on their own devices.

Under GDPR, written permission from parents or carers will be obtained before photographs of staff / students / pupils are published on the school website or in school social media sites. Please see Parent contracts and Taking,storing and using images of children policy and Taking, storing and using images of adults policy. Photographs published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with the above policies. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

St Peter's Preparatory School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. Incidents of misuse or suspected misuse must be dealt with by the School in accordance with the Safeguarding Policy.

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our policies on behaviour and Anti-Bullying Policy.

Complaints

As with all issues of safety at St Peter's Preparatory School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it.

Complaints should be addressed to the Head as per the School's complaints policy in the first instance, who will liaise with the Senior Leadership Team and undertake an investigation where appropriate. Please see the complaints policy for further information.

Incidents of, or concerns around, e-safety, will be recorded by the DSL in accordance with the school's Child Protection and Safeguarding Policy.

Revision History		
Date Revised	**Changes**	**Reviewed By**
29 Apr 2025	Added paragraph on emerging AI & deep fake risk as well as linked the policy to Martyn's Law.	Dan Morris (Dir. of Operations)