The Peterborough School

Online Safety Policy

Policy Reference:	7h Online Safety Policy
Review Date:	April 2024
Reviewed by:	Head of Pastoral Care
Next Review:	April 2025
Review Frequency:	Annual

Introduction

It is the duty of The Peterborough 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, hate, 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:

- Artificial Intelligence (AI)
- In App Chat facilities
- Cloud Storage
- Games Consoles
- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Photo and video sharing apps including live streaming
- Commenting on live streaming sites
- Video calls;
- Podcasting;
- Online communities via games consoles, smart TVs , watches or speakers; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable 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. This policy will provide guidance for the use of technology when using devices with the capacity to connect to the internet and transfer data**.** It is linked to the following school policies:

- Safeguarding and Child Protection
- Staff Code of Conduct;
- Health and Safety;
- Behaviour;
- Anti-Bullying;
- IT Acceptable Use Policy;
- [Data Protection];Data Protection Act 2018
- Bring Your Own Device; and
- PSHE.
- Whistleblowing?

Whilst exciting and beneficial both in and out of the context of education, many sources of 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.

We understand the responsibility to educate our pupils on Online 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 Online Safety and listening to their fears and anxieties as well as their thoughts and ideas.

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, governors, 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 Acceptable 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, etc.).

Roles and responsibilities

A whole school approach is taken when it comes to the responsibility of Online Safety. All staff are encouraged to find a way to embed online safety messages across the curriculum and out of classroom settings. More specific roles are as follows;

1. The Governing Body - is responsible for the implementation of this policy and for reviewing its effectiveness.

2. The Headmaster - is responsible for the safety of the members of the school community

3. The Designated Safeguarding Lead is responsible for Online Safety. The DSL delegates day-to-day management to the Head of Computing. In particular, the DSL ensures that:
    a. staff, in particular the Head of Computing are adequately trained about Online Safety; and
    b. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of Online Safety in connection to the school.

4. The Head of Computing - is responsible for the day to day issues relating to Online Safety. They are responsible for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current Online Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Safeguarding Children Partnership Board.

5. Computing staff - the school's technical staff have 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 and software systems, 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 Head of Pastoral Care/Head of Prep School in the case of pupils or the Headmaster for all other users.

6. Teaching and support staff - all staff are required to sign the IT Acceptable 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 Online Safety issues which may arise in classrooms on a daily basis.

7. Pupils - are responsible for using the School's IT systems in accordance with the IT Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

8. Parents and carers – the School believes that it is essential for parents to be fully involved with promoting Online Safety both in and outside of school. We regularly communicate with parents 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 IT Acceptable Use Policy.

Education and training

1. Staff: awareness and training

   New staff receive information on the School's Acceptable Use policy as part of their induction.

   All staff receive regular information and training on Online Safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety.

   All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

   Teaching staff are encouraged to incorporate Online 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 Online Safety occurs and be provided directly to the School's Safeguarding Lead via the School's online reporting system, MyConcern.

2. Pupils: Online Safety in the curriculum

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

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

   At age-appropriate levels, and usually via PSHE, pupils are taught about their Online Safety responsibilities and to look after their own online safety. From Year 7, pupils are formally 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 are taught to evaluate online content. Pupils are also taught about relevant laws applicable to using the internet; such as Computer Misuse Act, data protection and intellectual property. Pupils are taught about respecting other people's information, images, their rights and responsibilities as digital citizens

   Pupils can report concerns to the Safeguarding Lead or any member of staff at the school.

   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 their Form Tutor, Head of Key Stage/Key Stage Leader, Safeguarding Lead, as well as parents, peers and other School staff 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 Online 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 when they use electronic equipment at home. The School therefore arranges discussion evenings for parents when an outside specialist advises about Online Safety and the practical

steps that parents can take to minimise the potential dangers to their child without curbing their natural enthusiasm and curiosity. Our school newsletter also has a regular Online Safety section with tips, advise and conversation starters for parents.

4. Community

In February each year we celebrate the Safer Internet Day by putting on a range of activities that encourage the whole school community to have conversations about Online Safety. Where possible our activities are supported by Industry Experts who also give their time in supporting parent information sessions.

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. Devices issued to staff are encrypted, to protect data stored on them.

Staff at the School are permitted to bring in personal devices for their own use. They may use such devices in the staffroom or when privacy can be assured.

Personal telephone numbers, email addresses, or other contact details must 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 out of School messaging system.

Pupils

Pupils in the Prep School are not permitted to bring mobile devices to School. In exceptional cases, permission may be granted by the Head of Preparatory School, in which case the device must be handed in to Reception at the start of the day and collected as they leave School.

If Senior School pupils below Sixth Form bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day, stored within their locker, and will remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, excluding smartwatches which may be worn during the day.

For pupils in Years 10 to 13, the School has introduced the use of pupil owned devices as a teaching and learning tool and pupils are required to adhere to the Pupil BYOD Policy. In particular, the Pupil BYOD Policy requires pupils to ensure that their use of tablets for school work complies with this policy and the IT Acceptable Use Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the relevant Head of Key Stage or Senior Leader to agree how the School can appropriately support such use. The Head of Key Stage will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

General

All school issued devices are subject to monitoring for students and staff. Students who receive a device on the laptop scheme should be aware that devices will continue to be monitored when they leave the school site until the end of their agreement term. Please see The Peterborough School 1:1 Device Programme Policy.

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in staff-only areas of the School.

When accessed from staff members' own devices, staff must use social networking sites 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.

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that all School devices are monitored continuously using monitoring software.

Staff must immediately report to a member of the Senior Leadership Team 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 Bursar or Head of Computing without delay.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring the 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; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should pupils or parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Staff should not 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. However, it is understood that some staff may be personal friends with parents and this clause does not apply in those circumstances.

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/messaging service may be regarded as safe and secure, and must be used for all School work assignments / research / projects. Pupils should be aware that email communications through the School network and School email addresses are monitored.

Pupils should be aware that all School devices are monitored continuously using monitoring software.

There are strong security systems including; filtering, anti-virus 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 / research purposes, pupils should contact the IT Support 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 the Head of Computing or another 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 understand their responsibility to report any inappropriate online behaviour including accidental access to materials of a violent or sexual nature directly to the Head of Computing or another member of staff. 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 Policy. Pupils should be aware that all internet usage via the School's systems and its wifi network is monitored.

Specific details for Filtering and Monitoring:

Filtering

- User goes to website.
- Firewall inspects websites HTTP content and HTTPs content is decrypted to be checked. (Even secure websites are checked.)
- Firewall checks users' group to see if type of website/content/rules /country is allowed.The IT Dept can allow websites which are in countries that have been blocked)
- Firewall uses the firewall certificate to reseal/encrypt the files to be passed to the web browser if allowed.

Monitoring

- SECURUS software
- Monitors ALL activity on devices – not just internet
- Checked by DSL trained members of SLT

3. Data storage and processing

The school takes its compliance with the data protection legislation seriously. Please refer to the School's Data Protection Policies and the IT Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their School Microsoft Onedrive or School's central server.

Staff devices should be encrypted if any data or passwords are stored on them. The School discourages the use of all removable media (USB memory sticks, CDs, portable drives). Any removable media should be encrypted.

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 Bursar.

4. Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server and in Microsoft Onedrive. Staff and pupils are regularly reminded of the need for password security and will be asked to change their password periodically.

All pupils and members of staff should:

- use a strong password (Your password will need to be 9 characters long; you can use 3 random words to create a secret and unique password that is easy to remember e.g desklightrain; complexity can also be helpful by including a capital letter, number and special characters e.g *,!$,£), 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 are welcome to take videos and digital images of their 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 on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the IT Acceptable Use Policy and other relevant policies concerning 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.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the School website (see Parent Contract for more information).

Photographs published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

The Peterborough 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 Safeguarding Children Partnership Board. 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 staff in accordance with the School's policies and procedures.

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 Anti-Bullying and Behaviour Policies.

7. Responding to incidents and concerns

All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, cyberbullying and illegal content. All members of the community must respect confidentiality and investigations and debriefs will be carried out on a need to know basis.

Complaints

As with all issues of safety at The Peterborough School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to Online Safety prompt action will be taken to deal with it. Complaints should be addressed to the Head of Computing in the first instance, who will liaise with the Senior Leadership Team and undertake an investigation where appropriate. Please see the Complaints Policy and Procedure for further information, available on the School's website.