E-Safety Policy
April 2022

Introduction

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

The PHS E-safety coordinators are Gemma Simper and Tacita Crossland.

The *Education and Inspections Act 2006* empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off school sites and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school.

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 e-safety behaviour that takes place out of school.

The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated. The Principal is responsible for ensuring that the e-safety coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety role and to train other colleagues as relevant.

E-safety

The school will have a named member of staff with a day-to-day responsibility for e-safety. Their duties will include:

- taking a lead on e-safety
- taking day-to-day responsibility for e-safety issues
- ensuring that all employees are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- liaising with the Local Authority or any other relevant body

All employees are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school E-safety Policy and practices
- they report any suspected misuse or problem to the Principal for investigation/action/ sanction

- all digital communication with pupils/pupils/parents/carers should be on a professional level and only carried out using PHS systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-safety and Acceptable Use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations
- monitoring of the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre- planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable/inappropriate material that is found on the internet searches.

The **Designated Safeguarding Lead and Deputies** should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues which may arise from:

- the sharing of personal data
- accessing illegal/inappropriate materials
- inappropriate on-line contact
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school computer systems in accordance with the teachers guidelines set out in that lesson
- have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand the issues which may arise from taking and using images, and also from cyber-bullying
- should understand the importance of adopting good e-safety practice when using computers out-of-school.

Parents/ Carers

Many parents/carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and maybe unsure how to respond. Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, and the School website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events and their children's use of personal electronic devices in school

Curriculum

Whilst regulation and technical solutions are very important educating pupils in taking a responsible approach to the use of such devices is equally important. The education of pupils in e-safety is therefore an essential part of the schools e-safety provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and to build their resilience.

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

- A planned e-safety curriculum should be provided as part of computing/PHSE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the students and encouraged to adopt safe and responsible use both within and outside school.
- Employees should act as good role models in their use on computers, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found during internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked; staff can temporarily remove sites from the filtered list for the period of study.

Training

It is essential that all employees receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy.

Digital imaging

- 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 eg on social networking sites.

- Parents and 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 or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital image.
- Employees are allowed to take digital/video images to support educational aims, but most follow the schools policies with regards to sharing, distribution and publication of the images. The images should only be taken on school equipment. The personal equipment of staff **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 or publish images of others without their permission.
- Pupil's full names will not be used anywhere on a website – particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for a limited purpose
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subjects rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for
- every effort will be made to ensure that data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay
- risk assessments are carried out
- it has clear and understood arrangements for the security, storage and transfer of personal data
- data subjects have rights of access and there are clear procedures for this to be obtained
- there are clear and understood policies and routines for the deletion and disposal of data

Employees must ensure that they:

- take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices, ensuring that they are properly logged off at the end of any session in which they are using personal data

When personal data is stored on any portable computer system, memory stick or any other removable electronic media -

- The device must be password protected
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

When using computers, PHS considers the following as good practice -

1. The school email service may be regarded as safe and secure, staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
2. Users must immediately report any activity that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
3. Any communication between staff, pupils, parents/carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
4. Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using computers.
5. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

All schools and LAs have a duty of care to provide a safe learning environment for pupils and staff. Schools and LAs could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

PHS provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils and employees:

- by limiting access to personal information
- by ensuring that training includes acceptable use; social media risks, checking of settings; data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment

Staff should ensure that:

- no reference is made in social media to pupils, parents/carers or other school staff
- they do not engage in online discussions on personal matters relating to members of the school community
- personal opinions should not be attributed to the school

Actions

In any instance where an E-safety incident occurs the Incident Log should be filled out immediately (this log originates from the NSPCC E-safety online training) and the E-safety Coordinator made aware. Incident logs should be handed into the E-Safety Coordinator so it can be dealt with accordingly. If an Incident Log is filled in, this should then be recorded appropriately in the incidence log book.