POLICY NUMBER:
OWNER: NATASHA HILTON
DATE OF ISSUE/LAST REVIEW: NOV 2024
REVIEW DATE: AUGUST 2025

E-SAFETY POLICY

RATIONALE

Park House English School is committed to promoting and safeguarding the welfare of all students and an effective online safety strategy is paramount to this.

Park House English School online safety strategy are threefold:

1. To protect the whole School community from illegal, inappropriate and harmful content or contact;
2. To educate the whole School community about their access to and use of technology; and
3. To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

This policy applies to all members of the School community, including staff and volunteers, students, parents and visitors, who have access to the School's Technology whether on or off School premises, or otherwise use Technology in a way which affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

The following policies, procedures and resource materials are also relevant to the School's online safety practices:

- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Policy for Students
- Safeguarding Policy

These policies procedures and resource materials are available to staff.

This is a whole School policy.

ROLES AND RESPONSIBILITIES

ISP

ISP has overall responsibility for safeguarding arrangements within the school, including the school's approach to online safety and the use of technology within the school.

ISP is required to ensure that all those with leadership and management responsibilities at the school actively promote the well-being of students. The adoption of this policy is part of the proprietors response to this duty.

ISP will undertake an annual review of the school's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies.

POLICY NUMBER:
OWNER: NATASHA HILTON
DATE OF ISSUE/LAST REVIEW: NOV 2024
REVIEW DATE: AUGUST 2025

Principal and Senior Leadership and Management Team

The Principal has overall executive responsibility for the safety (including online safety) and welfare of members of the school community.

The Principal and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, as covered in our staff conduct policy.

Designated Safeguarding Leads (DSLs)

The Designated Safeguarding Leads (DSL) are members of staff from the Senior Team (SLT) and other areas of the school with lead responsibility for safeguarding and child protection.

The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding Policy.

DSLs should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

The DSLs will work with the IT Manager in monitoring Technology uses and practices across the school and assessing whether any improvements can be made to ensure the online safety and well-being of students.

The DSLs will regularly monitor the Technology Incident Log maintained by the IT Manager.

The DSL will regularly update other members of the SLT on the operation of the School's safeguarding arrangements, including online safety practices.

IT Manager

The IT Manager, together with his team, is responsible for the effective operation of the School's filtering system so that students and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

The IT Manager is responsible for ensuring that:

(a) the School’s Technology infrastructure is secure and, so far as is possible, is not open

to misuse or malicious attack;
(b) the user may only use the School's Technology if they are properly authenticated and authorised;
(c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;
(d) the risks of students and staff circumventing the safeguards put in place by the School are minimised;(e) the use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
(f) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

The IT Manager will report regularly to SLT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, s/he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Leadership Team (SLT).

The IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the DSL in accordance with the School's Child Protection & Safeguarding Policy and Procedures.

All staff

The school staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the school's policies and of safe practice with the students.

Staff are expected to adhere, so far as applicable, to each of the policies referenced above.

Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy.

Staff must have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices

Staff must have read, understood and signed the Staff Acceptable Use Policy / Agreement

Staff should ensure all digital communications with students / parents / carers should be on a professional Level

Staff have a responsibility to ensure online safety issues are embedded in all aspects of the curriculum and other activities

Staff must ensure students understand and follow the Online Safety Policy and acceptable use policies

Staff will teach students to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Staff must monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

In lessons where internet use is pre-planned students 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 in internet searches

Parents

The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The school expects parents to promote safe practice when using Technology and to:

(a) support the school in the implementation of this policy and report any concerns in line with the school's policies and procedures;
(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

If parents have any concerns or require any information about online safety, they should contact the DSL.

Students

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and 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 policies on the taking / use of images and on online-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's / school's Online Safety Policy covers their actions out of school, if related to their membership of the school

EDUCATION AND TRAINING

Students

The safe use of Technology is integral to the School's ICT curriculum. Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy).

Technology is included in the educational programmes followed in the EYFS in the following ways:

(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

(b) children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

(c) children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

(b) to be critically aware of content they access online and guided to validate accuracy of information;

(c) how to recognise suspicious, bullying, radicalisation and extremist behaviour;

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

(e) the consequences of negative online behaviour; and

(f) how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

School's Acceptable Use of ICT Policy for Students sets out the School rules about the use of Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology. Students are reminded of the importance of this policy on a regular basis.

Staff

Park House English School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

Induction training for new staff includes guidance on this policy as well as the Staff Code of Conduct, Email & Internet Policy and Professional Use of Social Media Guidelines Policy. Ongoing staff development training includes training on Technology safety together with specific safeguarding issues including cyberbullying and radicalisation.

Staff also receive data protection guidance on induction and at regular intervals afterwards.

The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the Park House English School overarching approach to safeguarding.

Parents

Information is available to parents via the school website. Additionally, we offer the opportunity for parents to attend School-based sessions on online safety on an annual basis.

Parents are encouraged to read the Acceptable Use Policy for Students with their son/daughter to ensure that it is fully understood.

Useful resources

There are useful resources about the safe use of Technology available via various websites including:

(a) http://www.thinkuknow.co.uk/
(b) http://www.saferinternet.org.uk/
(c) https://www.internetmatters.org/
(d) http://www.kidsmart.org.uk/
(e) http://www.safetynetkids.org.uk/
(f) http://www.safekids.com/
(g) http://parentinfo.org/

ACCESS TO THE SCHOOL'S TECHNOLOGY

Park House English School provides internet and intranet access and an email system to students and staff as well as other Technology. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and his/her team.

- Students and staff require a user names and passwords to access the school's internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their user names or passwords must report it to the IT Department immediately.

- No laptop, tablet or other mobile electronic device may be connected to the school network without the consent of the IT Manager. All devices connected to the school's network should have current and up-to-date

anti-virus software installed and have the latest OS updates applied. The use of any device connected to the school's network will be logged and monitored by the IT Support Department.

- The school has a separate Wi-Fi connection available for use by visitors to the school. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

Use of mobile electronic devices

- Park House English School has appropriate filtering and monitoring systems in place to protect students using the Internet (including email text messaging and social media sites) when connected to the school's network. Mobile devices equipped with a mobile data subscription can, however, provide students with unlimited and unrestricted access to the internet. In certain circumstances, a student may be given permission to use their own mobile device to connect to the Internet using the school's network. Permission to do so must be sought and given in advance by the adult in charge.

- All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

- Park House English School rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Students.

- The use of mobile electronic devices by staff is covered in the staff Code of Conduct. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

- Park House English School policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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.
- Permission from parents will be obtained before photographs of students are published on the school website / social media / local press.
- Parents 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 / made publicly available on social networking sites, nor should parents comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school devices.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such image

Communications

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

When using communication technologies the school considers the following as good practice:

● The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

● Users must immediately report, to the nominated person – in accordance with the school / school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

● Any digital communication between staff and students or parent (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

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

● Ensuring that personal information is not published

● Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

● Clear reporting guidance, including responsibilities, procedures and sanctions

● Risk assessment, including legal risk

School staff should ensure that:

● No reference should be made in social media to students, parents or school / school staff

● They do not engage in online discussion on personal matters relating to members of the school community

● Personal opinions should not be attributed to the school

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

Personal Use

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

PROCEDURES FOR DEALING WITH INCIDENTS OF MISUSE

At Park House School, students are allowed to bring mobile devices into school. If they choose to do so it is on the understanding that they agree with the following limitations on its use as set out in this document. The school also accepts no responsibility for items that are damaged or lost / stolen.

Staff, students and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

Misuse by students

Mobile devices and, in particular, the new generation of smart phones, such as the iPhone, now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet. These allow immediate access to email, searching for information on the internet and other functions such as access to social networking sites e.g. Facebook, twitter and blogging sites.

For many young people today the ownership of a mobile device (or devices) is considered a necessary and vital part of their life. When used creatively and responsibly mobile devices have great potential to support a student's learning experiences.

Parents and students should be clear that misuse of mobile devices will not be tolerated. The following are examples of misuse but are not exclusive. 'Misuse' will be at the discretion of the Headteacher (or other designated member of staff):

- general disruption to learning caused by students accessing or using devices in lessons
- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience such as on Facebook or YouTube
- bullying by text, image and email messaging
- students posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others

- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other students
- students phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised
- publishing photographs of vulnerable students, where this may put them at additional risk.

Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy).

Social Time: Acceptable Mobile Device Use

Corridors / Stairs / School buildings / outdoor spaces

The distraction of mobile devices whilst walking around the school site both inside and outside the building is hazardous and risks personal safety. Therefore:

- No phones or other devices should be used or be visible inside the school buildings.
- When moving around the school site (both inside and outside) devices should not be used.
- Headphones including wireless earphones (airpods etc.) should not be used nor visible in the school buildings, classrooms OR when walking around school site (both inside and outside)

Misuse of mobile technology will be dealt with in line with the school behaviour policy.

Misuse by staff

Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy.

Misuse by any user

Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the the Principal.

The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

Monitoring and review

All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the IT Manager.

The DSL has responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.

Consideration of the effectiveness of the School's online safety procedures and the education of students about keeping safe online will be included in the ISP annual review of safeguarding.

EVALUATION