PAPILLON HOUSE SCHOOL

ONLINE SAFETY POLICY

Writing and reviewing the online safety policy

The Online Safety Policy relates to other policies including those for ICT, Anti-bullying and for Child protection and Safeguarding.

- Alicia Rickman - Designated Safeguarding Lead is responsible for online safety.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the Senior Leadership Team and approved by the Management Team.
- The Online Safety Policy and its implementation will be renewed annually.
- The Online Safety Policy was revised by: Alicia Rickman Head Teacher in June 2017
- It was approved by the Management Team on: 18 September 2017

The aim of this Online Safety Policy is to ensure that the level of risk is not unacceptably high, and to empower staff, parents and children to identify concerns and to manage the risks. This takes into account each child's strengths, vulnerabilities and stage of development.

This policy aims to help staff with the following:

- To help adults that work with learners to do so safely and responsibly when using electronic devices.
- To clarify which behaviours constitute safe practice and which types of behaviour should be avoided by staff.
- To help staff, to understand the boundaries of acceptable behaviour.
- To mitigate the risk of having malicious or just misplaced allegations being made against staff.
- To support the Management Team and Senior leaders in establishing: policies, codes of behaviour and a workplace ethos that safeguards staff as well pupils at Papillon House School.
- To assist the Management Team in giving a clear message that unsafe or, even more so, unlawful behaviour is unacceptable and that where appropriate, disciplinary or legal action will be taken.

Teaching and Learning

Why Internet and Digital Communications are Important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the curriculum and a necessary tool for staff and pupils.
- The Internet will be used across the school to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The School will seek to ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and Internet at home.
- For children with social, familial, or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Viral protection will be updated regularly.

E-mail

- Pupils and staff may only use approved e-mail accounts on the School system.
- Pupils are not permitted to send emails at school, unless this is part of a planned programme of study which forms part of the curriculum and is fully supervised by staff.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Management Team will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photographs of individual children.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the Website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking and Personal Publishing

- Social Network sites and newsgroups are not allowed to be accessed at the School.
- Pupils and parents/carers will be advised that the use of social network spaces outside school brings a range of dangers for children and young people.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Lead.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and responsible.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school
- Staff mobile phones and similar devices are only permitted to be used for non-work purposes outside of lesson time, in the Staff Room or where agreed in advance with the Head Teacher.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Pupils are strongly discouraged from bringing their mobile phones, tablets or similar devices to school. If a pupil brings one to school, for instance because they have been using it to play games during a long taxi journey to school, it will be kept in the school office on arrival and pupils will not be allowed to access it during the school day
- Appropriate tuition in the social use of devices for texting and Snapchat, for example, will be provided on a need-to-know basis through the PSHE and SRE curriculum.

The use of mobile phones to communicate with learners and their families

Staff should not use their private mobile phones as a method of communication with learners at any time without specific consent and knowledge of the School Senior Leadership Team. This includes giving their personal home or mobile phone numbers to learners to allow those learners to contact them. Even then this contact should be for only clearly defined purposes agreed by senior management. It is also inadvisable that staff members use their own personal mobile phones to communicate with a learner's family. Staff members should use the school landline when onsite and ensure they take a school mobile phone with them on visits where this type of communication may occur. In the event that this is not possible, and in extremely rare cases, teaching staff and group leaders may need to use their own mobile phone for this purpose. It is strongly recommended the staff member changes their privacy settings on their mobile device to ensure their personal number is not given to the family. There is no situation where it would be deemed appropriate that a staff member would ever contact a learner's family through the use of instant message, including texts or iMessage, on a personal device.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the data Protection Act 1998.

Policy Decisions

Authorising internet access

- All staff must read and sign "Staff Code of Conduct for ICT" before using any school ICT resource.
- The School will maintain a current record of all staff and pupils who are granted access to the school ICT systems.
- Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the School will be asked to sign an "acceptable use of ICT resources" before being allowed to access the internet from the school site.

Assessing Risks

- The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Papillon House School cannot accept liability for the material accessed, or any consequences of Internet access.

Inappropriate Content and Online Behaviour

Some types of Internet material or content are considered inappropriate for staff to be accessing. It is a criminal offence to access/create/save some types of information from the Internet. Clearly all staff should not view, download or create inappropriate, illegal or criminal content. Any member of staff that does so should be aware that the sanctions that can be applied range from disciplinary to criminal. Access to the Internet in Papillon is always logged and can be monitored or retrospectively investigated. As a result staff should be alert to the possibility of accessing inappropriate and illegal material and take steps to avoid this. Any activity that is illegal would be a breach of civil law and could result in, upon conviction, having to pay damages /compensation to an individual or organisation that brought a case to court. Any activity that is a criminal offence, if proven in court, would lead to a criminal record and possible fines or imprisonment. The range of behaviours is clearly huge and cannot possibly be covered completely in this policy but some could be so serious as to constitute gross misconduct. Examples of inappropriate behaviour include but are not limited to:

- Making indecent, offensive, insulting or threatening comments about learners or colleagues through any online activity including email and social media
- Attempting to access pornography of any type on school devices
- Contacting learners on social networking sites
- Looking at content that promotes Extremism and Radicalisation

Although all these activities are unacceptable and may well lead to disciplinary action they are not all illegal or criminal. However, possessing or distributing indecent images of a person under 18 is a criminal offence. Even viewing such images on-line may well constitute possession even if not saved. Saving such images on a computer is classed as "creating" those images. All staff should be aware that in the case of any material that is illegal/criminal to possess, an investigation might lead to: criminal investigation, prosecution, dismissal and barring. The possession of material that is inappropriate, but legal can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

The School will monitor ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Policy is appropriate and effective.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

Community use of the internet

- All use of the School Internet connection by community and other organisations shall be in accordance with this policy.

Communications Policy

Introducing the Online Safety Policy to pupils

- Appropriate elements of the policy will be shared with pupils.
- Online safety rules will be posted in all networked rooms.
- Pupils will be informed that the network and internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as students become more mature and the nature of newer risks can be identified.

Staff and the online safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the online safety policy and agree to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage the filtering systems or monitor ICT will be supervised by senior Leaders or the management Team and have clear procedures for reporting issues.

Enlisting parents' support

- Parents and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the School website.
- The School will ask all new parents to sign the Parent/Pupil agreement when they register their child with the school.
- Parents should be given online safety training regularly with the focus on education and having an overview of tools to allow them to take control whilst not undermining trust.
- Often children do not wish to be constantly online but lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible, to interact with their children on the internet as well as provide other opportunities for learning and recreation.

This policy should be read in conjunction with all other relevant policies. In particular:

- Child Protection and Safeguarding Policy
- Anti-bullying Policy

This policy was reviewed and revised by Alicia Rickman Head Teacher in consultation with Katie Lonnborg Deputy Head and Liz Evans Head of Therapy.
It was reviewed and agreed by the Management Team on18 September 2017

Policy				
e-safety	Written	Alicia Rickman	Acting Head Teacher	September 2014
e-safety	Reviewed	Alicia Rickman	Head Teacher	September 2015
e-safety	Reviewed & Amended	Alicia Rickman	Head Teacher	September 2016
Online Safety (previously e-safety)	Reviewed & Amended	Alicia Rickman	Head Teacher	June 2017

Further review currently taking place with VWV (Solicitors) advising The Management Team. To be updated December 2017 as appropriate.