PAXTON ACADEMY
SPORTS AND SCIENCE
INDIVIDUALLY EXCELLENT, COLLECTIVELY BRILLIANT

E-Safety Policy

Policy Sign off

	Reviewer	Approver	Date
Reviewer / approver	Theresa Moses (Headteacher)	LAC	Spring (March) 22
Next Review			Spring 23

Related policies: Safeguarding

WLT WANDLE LEARNING TRUST

E-Safety Policy

This policy document should be read in conjunction with the safeguarding policy, anti-bullying policy and remote learning policy to ensure that e-safety is embedded across the school. This policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.
If a member of staff or a school visitor has a concern regarding E-safety, they must speak to a member of the safeguarding team without delay and the incident should then be logged on CPOMS.
The E-Safety lead is the Designated Safeguarding Lead: Theresa Moses (Headteacher).

Aims

E-Safety has become a vital part of essential learning for children. Children are using ICT from a very young age and they need to learn how to stay safe. At school provide children with opportunities to learn how to be safe with ICT in a controlled, safe environment before they take these skills home to use on less restricted mediums.

The philosophy of 'empowering children to stay safe' includes aims that children are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of school;
- secure, stable and cared for.

Paxton Academy aims to:

- protect and educate pupils and staff in their use of technology;
- have the appropriate mechanisms to intervene and support any incident where appropriate.

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, social media and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

As stated in the 2021 guidance for 'Keeping Children Safe in Education', the breadth of issues classified within e-safety is considerable, but can be categorised into four areas of risk:
Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Keeping Children Safe in Education, para. 124 (September 2021)

The Risks

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. At Paxton we are committed to providing pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk.

"While it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." Keeping Children Safe in Education, p. 97 (September 2019)

Overview

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- An e-Safety education programme for pupils, staff and parents.

Handling e-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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see appendix D)

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. (See data protection policy)

Internet access

- Access to the Internet will be under adult supervision to ensure pupils access specific, approved on-line materials.
- Pupils, parents and staff will be asked to sign and return a consent form. (EYFS & KS1 agreement see appendix A/Ks2 see appendix B/ parents see appendix C and for staff see data protection policy)
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- 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 effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

School network safety measures

The school maintains broadband connectivity through the LGfL. Additionally, the school has up-to-date antivirus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, staff and pupils are not able to download executable files and software. Unfortunately, there is the potential for inappropriate material to get through any filtering system. Any inappropriate site will be reported to the Designated Member of staff for Safeguarding and access to inappropriate sites will be blocked.

Social Networking

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will learn about sensible use and how to make their profiles private.
- Pupils will also learn about the report features to be used on social networking sites if they have any problems.
- We filter access to social networking sites unless a specific use is approved.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

Google Classroom & e-mail use

- Pupils may only use approved accounts on the school system where these have been set up by the SLT e.g. Google Classroom accounts, Scratch programming accounts etc.
- Pupils must immediately tell a teacher if they receive offensive communication on any online platform in school time.
- Pupils must not reveal personal details of themselves or others.
- All staff must use the Paxton approved staff e-mail for all school related e-mails.

School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- It is the policy of the school to not allow pupils surnames or for any photographs which clearly identify any pupil to be used on the school website without the parents/carers permission.
- Content on the school website must not infringe copyright or intellectual property rights through any content published on the website.
- Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience.

Mobile phones

- Pupils: Mobile phones are not allowed to be used during the school day and should not be taken on school trips including residentials.

Staff: Cameras on phones cannot be used to take or store photos of children, mobile phone calls are not allowed to be answered during lesson times and mobile phones should have a passcode enabled to prevent any personal information being obtained by pupils.
Mobile phones are allowed on school trips.

Cyber Bullying

Cyber bullying is when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else. The school will help prepare pupils for the hazards of using technology while promoting learning and social opportunities. Cyber bullying is a form of bullying but because it happens online or on mobile phones it can happen 24 hours a day, seven days a week. Any issues of Cyber Bullying will be dealt with in line with the Anti-Bullying Policy.

Peer on Peer Abuse

Peer on peer abuse can manifest itself in many ways and can include, but is not limited to, bullying (including prejudice based and discriminatory) cyberbullying, sexting, gender-based violence, sexual abuse, up skirting and hazing/initiation abuse. All staff should recognise that children are capable of abusing their peers (including online). It often manifests itself through the use of mobile devices and the internet. Peer on peer abuse is not tolerated at Paxton Academy and it should not be passed off as "banter" or "part of growing up". In the case of peer on peer abuse, our Safeguarding Policy and Anti-Bullying Policy should be invoked. Our Safeguarding Policy and this E-Safety Policy set out the procedures taken by the school to minimise the risk of peer on peer abuse, and the Safeguarding Policy clearly states how allegations of peer on peer abuse will be investigated and dealt with.

Prevent

In line with our commitment to minimise the risk of pupils being radicalised, pupils' use of school computers is monitored and pupils found searching websites or using criteria that would suggest an interest in terrorism/radicalisation are immediately reported to the safeguarding team via CPOMS. The matter will then follow the procedures set out in the safeguarding policy.

Sexting/Youth Produced Sexual Imagery

Sexting is when someone shares sexual, naked or semi-naked images of themselves or others, or sends sexually explicit messages. They can be sent on any device that allows you to share media and messages. Sexting can be seen as harmless by young people but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

Take an explicit photo or video of themselves or a friend
Share an explicit image/video of a child, even if it is shared between those of the same age
Possess, download or store an explicit photo/image or video of a child, even if the child gave their permission for it to be created

In the most recent guidance produced by the UK Council for Child Internet Safety, Sexting in Schools and Colleges Resource Pack, sexting is referred to as "youth produced sexual imagery", although KCSIE (September 2021) still refers to "sexting".
Incidents of "sexting" will be investigated and dealt with in line with the safeguarding policy.

Teaching of E-safety

" *Governing bodies and proprietors should ensure children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a balanced curriculum. This may include covering relevant issues through PSHE."* Keeping Children Safe in Education, (September 2019)

- Pupils will be informed that network and internet use will be monitored.
- Pupils will be reminded about safe use of ICT every half term.
- Pupils will learn about e-safety in computing lessons and PSHCE lessons. It will also be embedded in cross-curricular lessons. Additional lessons are provided when needed.
- Pupils are taught about our 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials immediately.
- We run parent workshops as a preventative measure for targeted year groups to learn about e-safety so that they can create safer opportunities at home.

School staff

All staff are responsible for promoting and supporting safe behaviours in classrooms and the wider school by following school e-safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. All staff should be familiar with the schools' E-Safety Policy and have to sign the Acceptable Use Policy (see data protection policy).

Monitoring, Evaluation and Review

The school will review this policy annually and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

Think before you click	
S 	I will only use the Internet in school with an adult present.
A 	I will only click on icons and links when I know they are safe.
F 	I will only send friendly and polite messages.
E 	If I see something I don't like on a screen, I will always tell an adult.

My name: _____

Appendix B

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will **only** use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will only use my logins and passwords and keep them secret.
- I will not upload inappropriate material to any computer.
- I am aware that some websites and social networks have age restrictions and I **should** respect this.
- I will only access the Internet with permission from a member of staff and I won't attempt to visit Internet sites that I know to be banned by the school.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will screen shot it and show and tell a teacher / responsible adult.
- I understand the school will check my google classroom account and may monitor the websites I visit.
- I will not use my mobile phone during the school day.
- I will not send rude/offensive or abusive messages/videos online via social media or text/email.
- I will not bring my mobile phone on school trips without permission from school.
- I know that if I do not follow this agreement, personal equipment can be confiscated by the school.
- I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
  I have read and understand these rules and agree to them.

Name: _____ *Signed:* _____

Date: _____

Appendix C **Use of digital images - photography and video**

To comply with the Data Protection Act 2018, we need your permission before we can photograph or make recordings of your daughter/son.

- Where showcasing examples of pupils work or achievements in either text or video form (both to an internal and external audience) we only use a child's first name, rather than their full name.
- Only images of pupils in suitable dress are used.
- Staff are not allowed to take photographs or videos on their personal equipment.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted as far as possible. Please contact the school office if you want to withdraw consent at any point.

Please tick the boxes that you give permission for:

☐ I give permission for my child to be photographed by a member of staff or another child as part of a learning activity or individual/class school photograph (e.g. photographs to be used on display boards around school/used to support lessons/stuck in exercise books)

☐ I give permission for my child to be photographed for the school website and school social media (e.g. Paxton Twitter account, Paxton Facebook account etc.)

☐ I give permission for my child's image to be used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators (e.g. school prospectus/teaching courses etc)

☐ I give permission for my child's image to be used by third parties that visit our school (e.g. newspaper/film crews, maths and English hub visitors/visiting teachers).

The School's Responsibilities:

Although the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies. However Paxton does use an educationally filtered service, restricted access email, appropriate teaching practice and teaches e-safety skills to all pupils.

If we have concerns about a child's e-safety, a member of staff will contact parents directly. Please support the school by promoting safe use of the Internet and digital technology at home and inform the school if you have any concerns over your child's e-safety.

Parent / Guardian signature: _____Date: ___/___/___

Appendix D

Consequences for inappropriate use of technology

Category A

- Use of non-educational sites during lessons
- Unauthorised use of mobile phone (or other new technologies) in lessons
- Use of unauthorised instant messaging / social networking sites
- Accidentally corrupting or destroying others people's data (e.g. deleting online books reviews/computer work etc)
- Accidentally accessing offensive material but informs a member of staff.

Action to take: Class teacher to deal with and inform the parent of child involved.

Category B

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Accidentally corrupting or destroying others' data without notifying a member of staff of it (e.g. deleting online books reviews/computer work etc)
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Action to take: AHT to deal with and inform the parent of child involved. Record on CPOMS.

Category C

- Deliberately corrupting or destroying someone's data (online books reviews/computer work etc)
- Deliberately violating privacy of others (e.g hacking into their account/using other people's passwords etc)
- Sending or making an email/message/social media text or video message that is regarded as harassment or of a bullying nature (one-off)
- Sending or making an email/message/social media text or video message that is regarded as offensive e.g. racist/sexist/homophobic etc. (one-off)
- Deliberately trying to access offensive material

Actions to take: SLT to inform the child's parents and parents of any child involved in the incident. Report on CPOMS.

Category D

- Continued sending or making email/message/social media texts or video messages of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Bringing the school name into disrepute (e.g. posting online videos in school uniform that are deemed inappropriate in content/ videoing and posting messaging whilst on the school grounds in school time).

Actions to take: Refer to SLT and CPOMS to be completed. SLT to speak to the child's parents and parents of any child involved in the incident. (Removal of equipment in school if needed.)

Other safeguarding actions: *If inappropriate web material is accessed:*

1. Secure and preserve any evidence if possible
2. SLT to ensure appropriate technical support filters the site

3. SLT Inform ICT technician and LGfL if needed & ensure inappropriate comments/material posted by the child/children is removed.