St Paul's Way

Education · Foundation · Trust

Title:	**E-Safety Policy at St Pauls Way Trust School**	
Source:	**SPWT**	
Review/Updated by:	**Hannora Loveday**	
Document Owner:	**Hannora Loveday**	
Date Approved:	**January 2015**	
Date of Review:	**January 2017**	
Advisory Committee:		
Approval Committee:	**Full Governing Committee**	
Publication:	**School Website**	**Intranet/FROG**
	☑	☑

E-SAFETY POLICY AT ST PAUL'S WAY TRUST SCHOOL

The overall aim of this policy is establish and maintain robust standards and safeguarding procedures for all members of the school community in the use of ICT-based technologies.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites (e.g. pro-anorexia/self-harm/suicide sites)
- Hate sites (including sites promoting radicalisation or violent extremism)
- Social media and website postings referring to the school and/or any members of its community
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber bullying in all forms (towards any members of the school community)
- Incitement to radicalisation or violent extremism
- Identity theft (such as 'hacking' of profiles on social media) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (e.g. amount of time spent online or gaming)
- Sending and receiving personally intimate images, also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

This policy sets clear expectations and procedures to minimise these risks. It applies to all members of the St Paul's Way community (including staff, students, volunteers, parents and visitors) who have access to and are users of school ICT systems, both within and outside of school.

The school has a responsibility to regulate the online behaviour of students when they are off the school site and can take disciplinary measures for inappropriate behaviour. This pertains to instances of cyber bullying and other e-safety incidents covered by this policy which are linked to membership of the school whether they take place in school or not. The school will inform parents of incidents of inappropriate e-safety behaviour.

This policy is linked to the school's policy on Acceptable Use of the Internet. All other school policies apply to all uses of the internet.

Roles & Responsibilities

Role	Key Responsibilities
Senior Leaders	• To take overall responsibility for e-safety provision and data security • To regularly review the school e-safety protocols within our overall safeguarding policies and procedures • To ensure that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as appropriate
Curriculum & Pastoral Leaders *(Heads of Faculty, Subject Leaders, Subject Drivers and Year Team Leaders)*	• To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum • To communicate regularly with SLT to discuss current issues and review incident logs • To raise awareness of e-safety issues with parents and support them in promoting e-safety with their children at home • To keep up-to-date with e-safety issues and legislation, and be aware of the potential for serious child protection and safeguarding issues to arise from: o sharing of personal data o access to illegal/inappropriate materials o inappropriate on-line contact with adults/strangers o potential or actual incidents of grooming o access to organisations promoting radicalisation or violent extremism, cyber bullying and use of social media
Network Manager	• To report any e-safety related issues that arise to the Safeguarding Officer • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack • To ensure the security of the school ICT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • To ensure that the school's policy on web filtering is applied and updated on a regular basis • To inform LGfL of issues relating to the filtering applied by the Grid • To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts • To keep up-to-date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To regularly monitor use of the network, Virtual Learning Environment (Frog), remote access and email and to report any misuse or attempted misuse to the Safeguarding Officer for further investigation • To ensure that all data held on students on the VLE (Frog) is adequately protected • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on students on the school machines have appropriate access controls in place
All staff	• To read, understand and help promote the school's e-safety policies and guidance, including the Acceptable Use Policy

	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide students carefully when engaged in learning activities involving online technology (including extra curricular activities) • To teach students strategies to critically evaluate all online content • To ensure that students know how to report any problems or concerns that they have when using the internet or related technologies • To report any suspected misuse or problem to the Safeguarding Officer, Network Manager or pastoral or curriculum leader as appropriate • To ensure that students are fully aware of research skills and of legal issues relating to electronic content such as copyright law and plagiarism • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To ensure that any digital communications with students should be on a professional level using school based systems where possible. If, in an emergency, a personal device is used, staff should withhold their phone number • To log off or lock a computer as appropriate

This policy will be posted on the school website and the VLE (Frog). It will also be included in the induction pack for new staff (including student teachers). Acceptable use agreements will be issued to the whole school community (usually on entry to the school) and will be discussed with students at the start of each year. Once signed, these agreements will be held in student and personnel files.

Reporting Concerns

Any safeguarding concerns should always be reported to the School Safeguarding Officer, following our school policy. Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Other issues may be raised with the Network Manager or the appropriate curriculum or pastoral leader.

All members of the school community are encouraged to be vigilant in reporting issues, knowing that they will be dealt with quickly and sensitively through the school's procedures. Support is actively sought from other agencies if needed in dealing with e-safety issues. This includes contacting the police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

Student e-safety curriculum

This school has a clear, progressive e-safety education programme as part of the computing curriculum and the PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy
- To be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be
- To know how to narrow down or refine a search
- To correctly reference research findings and to avoid plagiarising the work of others
- To understand how search engines work and to understand that this affects the results they see at the top of the listings
- To understand acceptable behaviour when using an online environment and email

- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- To understand why they must not post pictures or videos of others without their permission
- To know not to download any files – such as music files – without permission
- To have strategies for dealing with receipt of inappropriate materials
- To understand why and how some people will 'groom' young people for sexual reasons
- To understand how the internet can be used to 'groom' young people for radicalisation or extremist violence
- To understand the impact of cyber bullying, inappropriate text messages and trolling and know how to seek help if they are affected by any form of online bullying
- To know how to report any abuse, including cyber bullying, and how to seek help if they experience problems when using the internet and related technologies
- To be aware that they should report any problems experienced online or with their ICT use to an adult

Parent awareness and training

The school will offer a programme of advice, guidance and training for parents around issues of e-safety, including:

- Introduction of the Acceptable Use Agreements to new parents
- Information leaflets
- Suggestions for safe internet use at home
- Articles and links on the school website
- Provision of information about national support sites for parents

Related Policies & Protocols

This policy should be read in conjunction with:

- Acceptable Use of Internet Policy
- Anti-Bullying Policy
- Safeguarding Policy

This E-safety Policy also links to the IT infrastructure technical specifications and our data protection procedures.