Preston School

A Business & Enterprise Academy

ONLINE SAFETY POLICY

Staff Link:	Carly Stewart	**Issue:**	4
Governor Link:	Graham Pritchard	**Date:**	September 2016
Issue Status:	Approved	**Review:**	March 2017

Contents

1 Introduction

This policy applies to all members of the Preston School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are using the Preston School ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Principals to such an extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online (cyber) bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of Preston School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over the issues covered by the Behaviour Policy.

Preston 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 online behaviour that take place out of school.

2 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Preston School:

Online Safety Lead	Carly Stewart, Assistant Head of School Business and Enterprise
Online Safety Governor	Graham Pritchard
Safeguarding Officer	Helen Cullen, Vice Principal

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of this policy. This will be carried out by the Governors of the Support Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Lead.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering / change control logs.
- Reporting to relevant Governors Sub Committee (Business & Site).

Principal and Senior Leadership

- The Principal has a duty of care for ensuring the safety (including the Online

Safety) of members of the school community, although the day to day responsibility for Online Safety will be delegated to the Online Safety Lead.

- The Principal and (at least) another member 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.
- The Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal safety monitoring role. This is to provide the safety net and also support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- Leads the Online Safety Committee.
- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provides training and advice for staff.
- Liaises with the relevant body.
- Liaises with the school technical staff.
- Receives reports of Online Safety incidents and creates a log of incidents to inform future e- safety developments.
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant Governors meetings.
- Reports regularly to the Senior Leadership Team.

Network Manager and IT Support Team

The Network Manager and IT Support team are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required Online Safety technical requirements and any other relevant body Online Safety Policy that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering system is applied and updated on a regular basis.

- That they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant.
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal, Senior Leaders, and/or the Online Safety Lead for investigation, action or sanction.
- That monitoring software systems are implemented and updated as agreed.

Staff

Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the Principal, Senior Leadership Team, and/or Online Safety Lead for investigation, action or sanction.
- All digital communications with students, parents and carers should be on a professional level and only carried out using school systems.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the Online Safety and Acceptable Use (AUP) Policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They 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.

Child Protection and/or Safeguarding Officer

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 (cyber) bullying.

Online Safety Committee

Members of the Online Safety Committee will assist the Online Safety Lead with:

- The production, review and monitoring of the Online Safety Policy documents.
- The production, review and monitoring of the school filtering and requests for filtering changes.
- Mapping and reviewing the Online Safety curricular provision - ensuring relevance, breadth and progression.
- Monitoring network, Internet and incident logs.
- Consulting stakeholders - including parents/carers and the students about the Online Safety provision.
- Monitoring improvement actions identified through use of the SWGfL 360-degree safe self-review tool.

Students

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy.
- 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 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 and use of images and on online (cyber) bullying.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet and mobile devices in an appropriate way. Preston School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website/VLE and information about national/local Online Safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website and on-line student records.

- Their children's personal devices in the school (where this is allowed).

Community Users

Community users who access school systems, website or VLE as part of the wider school provision will be expected to agree to a Guest Acceptable Use Policy before using the school systems.

3 Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the school's Online Safety provision, identified in section 4. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant, and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum should be provided as part of Computing lessons and should be regularly revisited.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.
- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Students should be helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within school and outside school.
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices.
- In lessons where Internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and the processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted from time to time, for good educational reasons, students may

need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be audit-able, with clear reasons for the need.

Education – Parents

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring 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 may be unsure how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, newsletters, web site, VLE.
- Parents Evenings.
- High profile events (e.g. Safer Internet Day).
- Reference to the relevant web sites (e.g. www.swgfl.org.uk / www.saferinternet.org.uk / www.childnet.com).

Education - The Wider Community

The school will provide opportunities for members of the community to gain from the schools' online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school web site will provide Online Safety information for the wider community.

4 Online Safety Provision

The Online Safety curriculum is broad, relevant, and provides progression whole school. The table below outlines the current level of provision provided for students, including unit titles and resources used:

Year Group	Assembly	PSHE	ICT	Life Studies
Year 7	Online Safety,		Social Networking,	Let's Fight it

	Misuse and Online (cyber) bullying - #payitforward day. National Anti-Bullying Month. Internet Safety Day.		Protecting Personal Information, Online Grooming, Cyber Crime and Bullying.	Together (workshop – externally provided).
Year 8			Online (Cyber) bullying, Digital Citizenship, Sexting, Online Grooming, Social Networking and Video Chat.	
Year 9		No provision.	Cyber Safety, Child Sexual Exploitation, PREVENT – Radicalisation and Extremism.	
Year 10			Searching safely online, plagiarism, Data Protection Act 1998, Computer Misuse Act 1990, Copyright Designs and Patents Act 1998 and Acceptable Use Policy.	
Year 11				

5 Training

Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available for staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policies.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL, LA, or other relevant organisation).
- The Online Safety Lead will provide advice, guidance, and training to individuals as required.

Training – Governors

Governors should take part in Online Safety training/awareness sessions, with particular importance for those who are members of any subcommittee involved in technology, Online Safety, health and safety, or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, SWGfL, or any other relevant organisation.
- Participation in school training/information sessions for staff or parents (this

may include attendance at assemblies or lessons).

6 Technical - Infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school network infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Preston School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and password by the IT Support team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.
- Internet access is filtered for all users.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless system, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date antivirus software.
- An agreed network is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) on to the school systems.

7 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/carers, and students need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for online (cyber) bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or long term. It is common for employers to carry out Internet searches for potential and existing employees. The school will inform and educate users about these risks.

- 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).

- In accordance with guidance from the Information Commissioners Office (ICO), parents/ carers are welcome to take videos and images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). 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 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 equipment; the personal equipment of staff should not be used for such purposes.
- 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 in to disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the school website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

8 Incidents of Misuse and Sanctions

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

The incident will be dealt with by the Principal and Governors, in line with existing school policy, which might include reporting the incident to the police and the preservation of evidence.

Equally the school will follow the policies laid out in the safeguarding documentation and will

inform necessary member of staff immediately to ensure the safeguarding of our young people. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Incident	Referral to:						Sanction
	Class Teacher	AHoS/ HoS	SLT	Network Manager (monitoring access rights)	Police	Parents/ Carers	
Deliberately accessing or trying to access material that could be considered illegal.	✓	✓	✓	✓	✓	✓	E-Safe Log = 2 negatives + suspend account.
Unauthorised use of non-educational sites during lessons.	✓	✓		✓		✓	E-Safe Log = 2 negatives.
Unauthorised use of mobile phone / digital camera / other handheld device.	✓		✓			✓	E-Safe Log = 2 negatives + confiscate device.
Unauthorised use of social networking / instant messaging / personal email.	✓	✓		✓		✓	E-Safe Log = 2 negatives + SLT detention.
Unauthorised downloading or uploading of files.	✓	✓		✓		✓	E-Safe Log = 2 negatives + isolation.
Allowing others to access school network by sharing username and passwords.	✓	✓		✓		✓	E-Safe Log = 2 negatives + isolation.
Attempting to access or accessing the school network, using another student's / pupil's account.	✓	✓		✓		✓	E-Safe Log = 2 negatives + isolation.
Attempting to access or accessing the school network, using the account of a member of staff.	✓	✓	✓	✓		✓	E-Safe Log = 2 negatives + SLT detention.

Corrupting or destroying the data of other users.	✓	✓		✓		✓	E-Safe Log = 2 negatives + SLT detention.
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.	✓	✓	✓	✓	✓	✓	E-Safe Log = 2 negatives + SLT detention.
Continued infringements of the above, following previous warnings or sanctions.	✓	✓	✓	✓	✓	✓	E-Safe Log = 2 negatives + SLT detention.
Actions which could bring the school into disrepute or breach the BASICS.	✓	✓	✓	✓		✓	E-Safe Log = 2 negatives + SLT detention.
Using proxy sites or other means to avoid the school's filtering system.	✓	✓	✓	✓		✓	E-Safe Log = 2 negatives + suspend account.
Accidentally accessing offensive or pornographic material and failing to report the incident.	✓	✓		✓		✓	Re-brief student AUP.
Deliberately accessing or trying to access offensive or pornographic material.	✓	✓	✓	✓	✓	✓	E-Safe Log = 2 negatives + suspend account.
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	✓	✓	✓	✓	✓	✓	E-Safe Log = 2 negatives + suspend account.

9 Data Protection

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to far greater scrutiny in their care and use of personal data. Preston School has a comprehensive Data Protection Policy which should be referred to for further information.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it 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.
- All personal data will be fairly obtained in accordance with the "Privacy Notice"

and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy.
- If it is registered as a Data Controller for the purposes of the Data.

Protection Act (DPA) Staff must ensure that they:

- At all times 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.
- Transfer data using encrypted and secure password protected devices.

10 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Preston School has an Electronic Communications Policy which should be referred to for further information regarding the use of communications technologies.

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 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 parents/carers (email, chat, phone etc.) must be professional in tone and context.
- Students should be taught about Online 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 digital technologies.

11 Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, online (cyber) bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place and are governed by both the School’s Social Networking and Acceptable Use Policy for staff.

`

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

information:

- Training to include: 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/carers, or school staff (unless permitted).
- 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.

The school's use of social media for professional purposes will be checked regularly by the Safeguarding Officer and Online Safety Committee to ensure compliance with the relevant policies.

12 Monitoring and Review

The implementation of this Online Safety Policy will be monitored by the Online Safety Lead and the Online Safety Committee. This Online Safety Policy has been approved by the Governing Body (Business & Site Committee). It will be reviewed biennially.

Signed _____ Date _____

Name _____ **Chair of the Governing body**