



E-SAFETY POLICY

Key document details

Equality Impact Assessment required?	Yes
If yes, date of EIA	25/01/21
Ratified:	Summer2 2024
Approver:	TB
Next review:	Summer2 2027

E-SAFETY POLICY

Introduction

Schools within Pioneer Educational Trust are inclusive communities that aim to support and welcome all students and staff. This policy is part of the Trust's Statutory Safeguarding agenda. Any issues and concerns with online safety must follow the Trust's safeguarding and child protection processes.

Our aim is to ensure that we can protect and educate pupils and staff in their use of technology and have appropriate mechanisms to intervene and act in the case of any incident relating to technology where appropriate.

The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users;
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm, to themselves or others.

Background

Keeping Children Safe in Education outline the responsibilities that schools have to ensure appropriate levels of filtering and monitoring are in place.

In 2007 the government commissioned from Dr Tanya Byron a review of the risks that children face when using the internet and video games. Following publication of the review in 2008, Ofsted was asked, among other things, to evaluate the extent to which schools teach pupils to adopt safe and responsible practices in using new technologies.

Childnet's 2016 Cyberbullying Guidance shows schools how to embed cyberbullying in their anti-bullying work.

The Education Framework for a Connected World was created to support educators who work with children and young people to help them develop effective strategies for understanding and handling risk online. Resources are available for all staff on SharePoint.

To help parents tackle online issue or to support them in keeping their children safe, Internet Matters have produced a series of videos and online safety guides which are age appropriate and these can also be found on SharePoint. There are also helpful teaching resources, guides and resources available here <https://www.internetmatters.org/schools-esafety/secondary/teaching-resources/>

Common risks that young people and/or staff are likely to encounter:
(Please note that this is not an exhaustive list)

Content

- Exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); and substance abuse;
- Lifestyle websites, for example pro-anorexia, self-harm or suicide sites;
- Hate sites;
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming;
- Cyber-bullying in all forms;
- Identity theft (including 'fraud' (hacking Facebook profiles) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information;
- Digital footprint and online reputation;
- Health and well-being (amount of time spent online (internet or gaming));
- Sexting (sending and receiving of 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).

Why is this important?

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age:

- Girls are more likely than boys to feel under pressure to appear popular or attractive online, and girls aged 12-15 are more likely than boys to say they have experienced cyberbullying through a mobile phone and online;
- Despite the vast majority of young people stating that they are confident internet users and know how to stay safe online, there has been an increase in children with a social networking site profile that may be visible to people not known to them. New technology brings new opportunities and risks, and children may need help to assess potential risks and unintended consequences of their media use, and to make informed decisions about online activities and services.

Technology use and e-safety issues go hand in hand. Many incidents happen beyond the physical geography of the school and yet can impact on pupils or staff. Consequences for actions will apply even if they took place outside of school hours and on other premises.

Just because these environments are online makes them no less susceptible to potential harm compared to the physical world. This makes it vitally important that pupils and staff are fully prepared and supported to use these technologies responsibly.

Annual training for all staff is compulsory as part of safeguarding and child protection updates. It reflects the current research and advances in technology.

E-safety advice is offered to parents where guidance is shared. E-safety resources are offered to and available for parents and children. These can be found on SharePoint.

There is a planned and progressive e-safety programme of education delivered across all age groups in an age appropriate way. It is embedded throughout the school curriculum and is regularly reviewed.

This policy applies to all members of the Trust community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the IT systems, both in and out of the schools.

Pupil online safety curriculum

Each Trust school:

- Has a clear, progressive online safety education programme as part of the curriculum through computing, PHSE and thinking skills. This covers a range of skills and behaviours appropriate to their age and experience;
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through the pupil acceptable use agreement(s);
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensures pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

For pupils with SEND

For many young people with Special Educational Needs or Disabilities (SEND), the internet can be a place where they feel safe, calm and in control. Somewhere they can make friends without having to communicate face-to-face, and build a community which they may not have in their offline life. Whilst recognising the internet is a great resource which young people enjoy using, life online for a child with SEND may pose additional challenges that require careful management and support. Further advice and guidance can be found at <https://www.childnet.com/parents-and-carers/hot-topics/supporting-young-people-with-send-online>
<https://www.childnet.com/resources/star-send-toolkit>

Sexuality and Gender Identity

Not all children and young people feel comfortable talking to their parents or carers about their identity or sexuality and may not report any online hate or bullying due to fear of the family not being supportive. Young people who identify as LGBTQ+ may be more at risk of grooming and child sexual exploitation or being bullied.

Gender identity support for pupils can be found at:

<https://www.childline.org.uk/info-advice/your-feelings/sexual-identity/transgender-identity/>

Coming out support can be found at:

<https://www.childline.org.uk/info-advice/your-feelings/sexual-identity/coming-out/>

Trans and homophobic bullying advice and guidance can be found at:

<https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/homophobic-bullying/>

Radicalisation, religion and belief

Children can be exposed to different views and receive information from various sources. Some of these views may be considered radical or extreme. Radicalisation is the process through which a person comes to support or be involved in extremist ideologies. It can result in a person becoming drawn into terrorism and is in itself a form of harm. Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. It includes calls for the death of members of the British armed forces (HM Government, 2011).

Further advice and guidance can be found at:

<https://learning.nspcc.org.uk/safeguarding-child-protection/radicalisation>

<https://learning.nspcc.org.uk/safeguarding-child-protection/for-faith-communities/about-safeguarding-in-faith-communities>

Roles and responsibilities

CEO

- To be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant; multi-agency safeguarding partnership guidance;
- To take overall responsibility for data management and information security ensuring the Trust's provision follows best practice in information handling;
- To ensure the schools within the Trust use appropriate IT systems and services including, filtered Internet Service;

- To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager.

Head

- To be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant multi-agency safeguarding partnership guidance;
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding;
- To take overall responsibility for online safety provision;
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles;
- To be aware of procedures to be followed in the event of a serious online safety incident;
- To ensure suitable consideration is given to the curriculum content around Online Safety and to ensure it meets the needs of pupils, including any risk of children being radicalised;
- To ensure school website includes relevant information.
- To ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety. (This is done via the calendar for monitoring and safeguarding governor visit feedback.)

Online safety coordinator/designated safeguarding lead (DSL) or deputy DSL working with Associate Director of Safeguarding in the Trust

- To take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents;
- To promote an awareness and commitment to online safety throughout the school community;
- To ensure that online safety education is embedded within the curriculum;
- To liaise with school technical staff where appropriate;
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
- To ensure that online safety incidents are logged as a safeguarding incident;
- To facilitate training and advice for all staff;
- To be regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.

Governors/safeguarding governor (including online safety)

- To ensure that the school has in place policies and practices to keep the children and staff safe online;
- To approve the online safety policy and review the effectiveness of the policy;
- To support the school in encouraging parents and the wider community to become engaged in online safety activities.

Computing curriculum leader

- To oversee the delivery of the online safety element of the computing curriculum.

Teachers

- To embed online safety in the curriculum;
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant);
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

Data and information manager

- To ensure that the data they manage is accurate and up-to-date;
- To ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements;
- To ensure that the school is registered with the Information Commissioner.

Network management

- To report online safety related issues that come to their attention, to the DSL/DDSL;
- To manage the school's computer systems, ensuring:
 - school password policy is strictly adhered to;
 - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date);
 - access controls exist to protect personal and sensitive information held on school-owned devices;
 - the school's policy on web filtering is applied and updated on a regular basis.
- To monitor the use of school technology and online platforms regularly and report misuse/attempted misuse to the online safety co-ordinator/CEO/Head of School;
- To ensure appropriate backup procedures and disaster recovery plans are in place;
- To keep up-to-date documentation of the school's online security and technical procedures.

Pioneer Educational Trust:

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the systems administrator/network manager and technical support are up-to-date services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Ensures storage of all data within the schools conformss to and UK data protection requirements.

To ensure the network is used safely, each Trust school:

- Issues pupils with their own unique username and password which gives them access to the internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities;
- Maintains equipment to ensure health and safety is followed;

- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Uses secure data transfer;
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA;
- Has a wireless network has been secured to appropriate standards suitable for educational use;
- Has IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private;
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

Handling incidents

- The school will take all reasonable precautions to ensure online safety;
- Staff and pupils are given information about infringements in use and possible sanctions;
- Online safety coordinator acts as first point of contact for any incident;
- Any suspected online risk or infringement is reported to online safety coordinator that day;
- Any concern about staff misuse is always referred directly to the CEO/Head, unless the concern is about the CEO in which case the complaint is referred to the Chair of Trustees and the LADO (Local Authority's Designated Officer) where appropriate. Please also see the Staff Code of Conduct.

Trust / school websites

- The CEO/Head, supported by the governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The schools' websites must comply with statutory DFE requirements.

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into a Trust school are entirely at the staff member, students & parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school. They remain the responsibility of the device owner;
- No students should ever be using his or her mobile phone or personally-owned device in school without permission. Any device used inappropriately in school will be confiscated;
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets 'Mobile and camera-free' signs to this effect are displayed;
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent;
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned;
- All visitors are requested to keep their phones on silent;

- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, such as pornography, violence or bullying etc;
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Review and monitoring

The online safety policy is referenced within other school policies (e.g. safeguarding and child protection policy, behaviour policy, PSHE, computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Trust schools;
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by governors. All amendments to the Trust school's online safety policy will be disseminated to all members of staff and pupils.