Pioneer Educational Trust
aspire inspire

Pioneer Educational Trust

aspire inspire

E-SAFETY POLICY

Key document details

Ratified:	**October 2017**
Approver:	**Trust Board**
Next review:	**October 2020**

Pioneer Educational Trust
aspire inspire

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.

Recommendations for schools

The report recommended that schools:

- Audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies;
- Work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school;
- Use pupils' and families' views more often to develop e-safety strategies;
- Manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school and provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies;
- Work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe;
- Systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.

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 'frape' (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).

Content, contact and conduct exemplars:

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online

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 sessions are offered to parents where advice and guidance is shared. E-safety resources are offered to and available for parents and children.

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.

Roles and responsibilities

CEO

- To be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance;
- To take overall responsibility for data management and information security (SIRO) 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 of School

- To be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) 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 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised;
- To receive regular monitoring reports from the pastoral lead at the school who will also act as the on-line safety coordinator/ DSL;
- To ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety;
- To ensure school website includes relevant information.

Online safety coordinator/designated safeguarding lead (DSL) or deputy DSL working with the strategic lead for 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 communicate regularly with SLT and the designated online safety governor/committee to discuss current issues, review incident logs and filtering/change control logs;
- 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 oversee any pupil surveys / pupil feedback on online safety issues;
- To liaise with the Local Authority and relevant agencies;
- 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;

The role of the online safety governor will include: regular review with the online safety co-ordinator.

Computing curriculum leader

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

Network manager/technician

- To report online safety related issues that come to their attention, to the online safety coordinator;
- 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 keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- 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.

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.

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.

All staff, volunteers and contractors

- To read, understand, sign and adhere to the school staff acceptable use agreement/policy, and understand any updates annually. The AUP is signed by new staff on induction;
- To report any suspected misuse or problem to the online safety coordinator;
- To maintain an awareness of current online safety issues and guidance e.g. through CPD;
- To model safe, responsible and professional behaviours in their own use of technology.

Exit strategy

At the end of the period of employment/volunteering, to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

User responsibilities

Pupils

- To read, understand, sign and adhere to the student/pupil acceptable use policy annually;
- To understand the importance of reporting abuse, misuse or access to inappropriate materials;
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the Trust's online safety policy covers their actions out of school;
- To contribute to any 'pupil voice' / surveys that gathers information of their online experiences.

Parents/carers

- To read, understand and promote the school's pupil acceptable use agreement with their child/ren;
- To consult with the school if they have any concerns about their children's use of technology;
- To support the school in promoting online safety and endorse the parents' acceptable use agreement which includes the pupils' use of the internet and the school's use of photographic and video images.

External groups including parent groups

- To sign an acceptable use agreement prior to using technology or the internet within school;
- To support the school in promoting online safety;
- To model safe, responsible and positive behaviours in their own use of technology.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website;
- Policy to be part of school induction pack for new staff;
- Regular updates and training on online safety for all staff;
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

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 of School, unless the concern is about the CEO in which case the compliant is referred to the Chair of Trustees and the LADO (Local Authority's Designated Officer).

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.

Pupil online safety curriculum

This 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.

Staff and governor training

This Trust school:

- Makes regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safety policy and the school's acceptable use agreements.

Parent awareness and training

This Trust school:

- Provides induction for parents which includes online safety;
- Runs a rolling programme of online safety advice, guidance and training for parents.

Expected conduct

In this Trust school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant acceptable use agreements;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- Know and understand school/Trust policies on the use of mobile and hand held devices including cameras.

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open internet searching is required with younger pupils.

Parents/Carers

- Should provide consent for pupils to use the internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this Trust school:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- Support is actively sought from other agencies as needed in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – police and LA will be informed.

Internet access, security (virus protection) and filtering

This Trust school:

- Informs all users that internet/email use is monitored;

- Has the educational filtered secure broadband connectivity through Virgin Media;
- Uses the lightspeed filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant;
- Ensures network health through use of Microsoft EndPoint anti-virus software;
- Uses approved systems including Egress secure file/email to send 'protect-level' (sensitive personal) data over the internet;
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

Network management

This Trust school

- 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 is 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:
- Storage of all data within the school will conform to the EU and UK data protection requirements;

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

- Ensures staff read and sign that they have understood the school's online safety policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network /we also provide a different/use the same username and password for access to our school's network;
- 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.

Password policy

- This Trust school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private;
- We require staff to use STRONG passwords;
- We require staff to change their passwords regularly.

E-mail

This Trust school

- Provides staff with an email account for their professional use;
- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up to date.

Pupils:

- Are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Will use e-mail systems for professional purposes;
- May have, access in school to external personal e mail accounts blocked;
- 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;
- Will only contact students or their families through the school system and the school email account.

Trust school's website

- The CEO/Head of School, supported by the governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate;
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Head of School;
- 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 /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work;
- Students are required to sign and follow our [age appropriate] pupil acceptable use agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental acceptable use agreement and additional communications materials when required;
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

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;
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day;
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices;
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned;
- Staff members may use their phones during school break times;
- All visitors are requested to keep their phones on silent;

- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the CEO/Head of School. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the CEO/Head of School is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary;
- 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. Staff mobiles devices may be searched at any time as part of routine monitoring;
- 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 are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting;
- 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.

Digital images and video

In this Trust school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually);
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's acceptable use policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.