Education Partnership Trust

Creating outstanding schools which transform learning, lives and communities

E-SAFETY POLICY

Document Control

This document has been approved for operation within:	All Trust Establishments
Date effective from	November 2023
Date of next review	November 2025
Review period	2 years

CONTENTS

1.0 AIMS

1.1 The school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile phones and other smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.

2.0 LEGISLATION AND GUIDANCE

2.1 This policy is based on the Department for Education's (DfE) statutory Safeguarding guidance, Keeping Children Safe in Education 2021, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

2.2 It also refers to the Department's guidance on protecting children from radicalisation.

2.3 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

2.4 The policy also considers the National Curriculum computing programmes of study.

3.0 ROLES AND RESPONSIBILITIES

Trust

3.1 The Trust has overall responsibility for the effective operation of this policy and ensuring compliance with the relevant statutory or Trust framework. The Trust has delegated day to day responsibility for operating the policy to the Headteacher.

3.2 The Local Governing Body is consulted on the policy.

3.3 The Senior Leadership Team in school has a specific responsibility to ensure fair application of this policy and all members of staff are responsible for ensuring its success.

The Governing Board

3.4 The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

3.5 The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

3.6 The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

3.7 The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.8 The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

3.9 The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

3.10 All governors will:

- Ensure they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet;
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Designated Safeguarding Lead

3.11 Details of the school's DSL and deputy DSLs are set out in our Safeguarding Policy.

3.12 The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the ICT Security & Safeguarding Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the EPT Behaviour Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing body
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The ICT Manager

3.13 The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems 24/7.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the EPT Behaviour Policy.

All staff and volunteers

3.14 All staff, including contractors, agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2) and ensuring that pupils follow the school's terms on acceptable use (Appendix 1) Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the EPT Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'(see Anti-Bullying Policy)

Parents

3.15 Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding online safety.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

3.16 Further guidance on keeping children safe online can be found on the useful links section

Visitors and members of the community

3.17 Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2). Visitors and members will be given a temporary and monitored account when using ICT equipment and accessing the internet to ensure no inappropriate behaviour is taking place.

4.0 EDUCATING PUPILS ABOUT ONLINE SAFETY

4.1 Pupils will be taught about online safety as part of the National Curriculum:
All schools will teach:

- Relationships education and health education to primary aged pupils.
- Relationships and sex education and health education in AP/SEMH & Secondary schools.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

4.2 In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Only use school IT equipment or other technologies for educational purposes.

4.3 Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.
- Only use school IT equipment or other technologies for educational purposes.

4.4 In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.
- Only use school IT equipment or other technologies for educational purposes.

4.5 Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.
- Only use school IT equipment or other technologies for educational purposes.

5.0 EDUCATING PARENTS ABOUT ONLINE SAFETY

5.1 The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents via the website.

5.2 Online safety will also be covered during parents' evenings.

5.3 If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

5.4 Concerns or queries about this policy can be raised with the DSL or the Headteacher.

6.0 CYBER-BULLYING

Definition

6.1 Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the EPT Behaviour Policy.)

Preventing and addressing cyber-bullying

6.2 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness as well as the victim.

6.3 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

6.4 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6.5 All staff and volunteers (where appropriate) will receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

6.6 The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

6.7 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Behaviour Policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is dealt with.

6.8 The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

6.9 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads, and other tablet devices, where they believe there is a 'good reason' to do so.

6.10 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

6.11 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police
- Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

6.12 Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

6.13 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure (See Complaints Policy).

7.0 ACCEPTABLE USE OF THE INTERNET IN SCHOOL

7.1 All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

7.2 The use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

7.3 We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

7.4 More information is set out in the acceptable use agreements in appendices 1.

7.5 Any breach of the terms will be dealt with inline with the ICT Security Policy.

8.0 PUPILS USING MOBILE DEVICES IN SCHOOL.

8.1 Pupils may bring mobile devices into school but are not permitted to use them.

8.2 Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

8.3 Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Behaviour Policy, which may result in the confiscation of their device.

9.0 STAFF USING WORK DEVICES OUTSIDE SCHOOL

9.1 Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

9.2 Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

9.3 If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

9.4 Work devices must be used solely for work activities. Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 1.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing any anti-virus and anti-spyware software recommended by the school.
- Keeping operating systems up to date – always install the latest updates.
- VPN to ensure safe connection when using public networks or private networks. IT team at the school will ensure this is setup on staff devices.

10.0 HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE.

10.1 Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and ICT Security Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

10.2 Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff

disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

10.3 The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11.0 TRAINING

11.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

11.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

11.3 The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

11.4 Volunteers will receive appropriate training and updates, if applicable.

11.5 More information about safeguarding training is set out in our EPT Safeguarding Policy.

12.0 MONITORING ARRANGEMENTS

12.1 The DSL logs behaviour and safeguarding issues related to online safety.

12.2 This policy will be reviewed every 2 years by the Trust. At every review, the policy will be shared with the governing body for consultation.

13.0 LINKS WITH OTHER POLICIES

13.1 This online safety policy should be read in conjunction with:

- Child Protection and Safeguarding policy
- Behaviour Policy
- Anti-Bullying Policy
- Data protection Policy and Privacy Notices
- ICT Security Policy

14.0 USEFUL WEBSITES

Keeping Children Safe in Education 2023

UK Safer Internet Café

Childnet – help and advice for parents and carers

Appendix 2 – Acceptable use agreement Staff/Visitors

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the School Business Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature _____ Date _____

Full Name (Print) _____ Job title _____