

June 2024



E-SAFETY POLICY

**HORIZONS EDUCATION TRUST
AMERICAN LANE, HUNTINGDON, CAMBRIDGESHIRE. PE29 1TQ**

DOCUMENT CONTROL	
ISSUED	CHANGES FROM PREVIOUS VERSION
Date reviewed: June 2024 Date of next review: June 2026 Reviewer: KT Date of ratification by Governing Board:	

Context:

Horizons Education Trust believes that the use of information and communication technologies not only creates opportunities for our young people but brings great benefits to their lives as well. However, with these opportunities are a number of associated risks. Our schools recognise the safeguarding issues and continue to work to develop our policy and plan to minimise these risks accordingly. We have used materials found at www.esafety.cceducation.org and www.theictservice.org.uk to help us produce an action plan.

E- Safety in schools is a child safety and not an ICT issue. Therefore this policy should be viewed alongside other Safeguarding policies including those for behaviour, anti-bullying, personal, social and health education (PSHE) and for citizenship. In addition all staff and volunteers have received a copy of, and training for, 'Keeping safe in Education'.

Contents

- The background to this policy
- Rationale
- Teaching and Learning Using Online Technologies
- Technology in School
- Staff and Student expectations
- The E- Safety Curriculum (Responsive curriculum)
- Safeguarding Children Online
- Responding to Incidents

Background to the policy

The purpose of this policy is to describe the safeguarding measures in place for children, young people and adults who are part of Horizons Education Trust:

- The ground rules we require at Horizons Education Trust for using the Internet and online technologies and how these fit into the wider context of our other Academy policies
- The methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Links to Fundamental British values and PREVENT

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the Academies share with parents and carers.

At Horizons Education Trust, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents. All our pupils have special education needs and as such are vulnerable to child sexual exploitation and abuse.

The development of our safety policy involved the following steps:

- Circulation to staff for comments.
- Copy to parent governors for their advice for suggestion of amendment.
- Adaptations and amendments from previous policies, reflecting the current social climate.

We have considered the following points:

- How children use technology in school
- What range of equipment they use
- Risks and concerns (Byron Review – 3 C’s ref.)
- Getting the balance between benefits and risks right
- Supporting children as they learn safe lifelong behaviours at home and school

At Horizons Education Trust we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming or exploitation by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication/contact with others, in the case of children and vulnerable young people and adults including strangers outside the scope of supervision by parents or adults with parental responsibility. In the case of staff or volunteers inappropriate communications that contravene the Acceptable use policy and therefore deem these adults as posing a risk to pupils.

- Cyber-bullying. We particularly ask staff to be vigilant for coercive behaviours.
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive internet use which may impact on the social and emotional development and learning of the young person. We alert staff to recognize that excessive internet use can lead to social isolation of vulnerable children, young people and adults.

While all children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them.

E-Safety issues can also affect adults who work or are associated with the school. For example Academy and personal data being entered on web/social networking sites, fraudulent email traps and cyber bullying.

It is impossible to eliminate risk completely. It is therefore essential, through our quality educational provision to manage the risk and deal with any threat to safety for all concerned.

Teaching and Learning Using Online Technologies

We have considered and continue to discuss the following issues:

- Watch the video- Shift Happens
- The importance of the internet to teaching and learning.
- The technologies used to access the internet
- The studies and government projects that highlight the educational benefits of appropriate internet use to increased pupil attainment.
- What regular e-safety education activity we might plan termly.

The internet is a part of everyday life for education, business and social interaction. Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the National Education Network (NEN) <http://www.nen.gov.uk/> connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

When using online technologies, it is essential that children, young people and adults understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. Due to the vulnerabilities of our special needs children and adults at Horizons Education Trust we need to ensure adequate supervision is part of any activity planned and staff assume responsibility for adult support and protection in line with the best endeavours of parents.

At Horizons Education Trust we believe that a comprehensive programme of planned e-safety education is vital for developing our pupils' ability to use technologies safely. We consider this can be achieved using a combination of discrete and embedded activities we have drawn from a selection of appropriate materials (see appendices).

We believe our children will learn safe life-long online behaviours by accessing and using the internet with reliable adult support. Members of staff constantly monitor pupils' use of the internet and other technologies. Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.

Messages to our vulnerable children, young people and adults involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's Acceptable IT Use Policy (see appendices).

Use of technology for online/virtual teaching

Schools in Horizons Education Trust use Microsoft Teams for online learning. Staff must use Academy devices and contact pupils only via the pupil email address/login. This ensures the appropriate filtering and monitoring software is enabled.

In deciding whether to provide virtual or online learning for a pupil, teachers should take into account issues such as accessibility within the family home and the mental health and wellbeing of children including screen time. Virtual lessons should be timetabled and senior staff DSL and/or heads of department should be able to drop in to any virtual lesson at any time.

Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

The following points should be considered:

- Think about the background, photos, artwork, identifying features, mirrors – the backing should be nondescript and ideally blurred.
- Staff and pupils should be in living/communal areas – no bedrooms.
- Staff and pupils should be appropriately dressed.
- Filters at a child's home may be set at a threshold which is different to the school.
- Resources/videos must be age-appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content.

It is the responsibility of the staff member to tact as moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and/or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching considerations should be given to data protection issues; e.g. whether parental/pupil consent is needed and retention/storage. If the staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately,

Staff should not contact a pupil or parent using their own phone. Academy phones are available.

Technology at Horizons Education Trust

We have considered and continue to discuss the following points:

- The infrastructure in school
- The range of technologies – fixed and mobile used by staff and children – and others?
- How inappropriate material is blocked or filtered.

Each school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service.

E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service.

Ref: E2BN Website

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and e-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders at Horizons Education Trust include:

Staff:

- Laptops and desktops/ tablets
- Cameras and video cameras,
- Internet, E-mail, Microsoft Office including Teams, central hosting including access to SIMS, and confidential pupil information

Pupils:

- Laptops and desktops/iPad
- Cameras and video cameras
- Internet, YouTube
- Other peripherals such as programmable toys, data loggers and control technology equipment

Others on Academy premises: Limited access to school systems such as filtered internet access using a visitor login.

Pupils login to our school network using an assigned class login and password.

All members of staff have individual, password protected logins to the school network and visitors to the Academies can access part of the network using a generic visitor login and password if agreed by the Head Teacher. Staff are required to update and change their passwords regularly. Staff laptops are Encryption protected and a password is required to gain access to individual login pages.

The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by Cambridgeshire Local Authority and the wireless key is kept securely by the Academy office. Academy staff and pupils are not permitted to connect personal devices to the school's wireless network and the wireless key is not given to visitors to the school.

E-safety expectations

All staff are expected to:

- Abide by the Data Protection Act
- Not access the schools wireless connection
- Lock computing devices away during the school day including mobile phones (expect in exceptional circumstance granted by SMT)
- Follow the ICT acceptable use policy
- Attend provided e-safety training
- Report any issues or concerns immediately
- Monitor students whilst they use computing devices (ensuring privacy settings are enabled and enforced)

All Students are expected to:

- Explore e-safety within the curriculum
- Abide by Horizons Education Trust Rules for Safer Internet Use policy
- Leave computing devices at home (expect in exceptional circumstance granted by SMT)
- Made aware of the consequences of computing and e-safety misuses. Both internal and external ramifications.

The E - Safety Curriculum

In line with recommendations in the E- Safety briefings for Ofsted we have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies. These opportunities include:

- Specific activities during e- safety days and anti-bullying week
- Age-relate classroom activities using the www.theictservice.org.uk materials
- Related work in PSHE lessons
- Posters and reminders in and around the school
- Schools own rules for safer internet use displayed within all classrooms.

Responsive Curriculum

At Horizons Education Trust we expect the e-safety and computing curriculum to adapt and develop in line with society. Tackling current and arising issues, respond to new and advanced technologies and criminal avenues of exploration.

When new software and trends occur, such as snapchat, WhatsApp, Instagram, gaming chat rooms, sexting, emoji's, etc... staff and parents need to be made aware of these issues. This can be communicated through regular meetings, training, Academy website, email or staff newsletter.

It is the responsibility of SMT, and the computing coordinator to ensure regular training and support is available for all staff and parents.

Safeguarding Children Online

In writing this section we have considered and continue to discuss:

- What age appropriate measures does the Academy need to consider to meet the needs of vulnerable children with special educational needs.
- What potentially harmful or inappropriate material could/have children encounter/ed.
- Do we need AUP's/rules and sanctions for different age groups or can one set of rules apply as decided to this point.
- How does the Academy respond to any incidents when a child's safety is at risk and notify as a child protection concern.
- Does our Academy conduct a risk assessment for new/ unknown situations.

Our Academy accepts that different users, whether children or adults, will be expected to use the school's technology systems in different ways – appropriate to their age, IT capabilities, disabilities or role in school. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children. UKCCIS (The UK Council for Child Internet Safety)

The Academy has published an Acceptable Use Policies (AUP) for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. Please see appendices for full details.

Any known or suspicious online misuse or problem will be reported to the Head Teacher for investigation/ action/ sanctions.

Responding to Incidents:

At Horizons Education Trust we renew staff training to show the vital importance that all members of staff have awareness of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. Any report of risk of harm to pupils must be reported using the Log of concern form (Blue) and provided to the Head Teacher who is the lead person in the Academy for safeguarding.

In the case of staff issues reported, the Head Teacher will follow the procedure for allegations against staff and may apply Disciplinary Rules sanctions which could lead to staff dismissal if deemed appropriate for staff who contravene the Acceptable use

Policy.

If an e-safety incident occurs Horizons Education Trust will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).

Where the Academy suspects that an incident may constitute a Child Protection issue, Child Protection procedures will be followed.

The Academy will evaluate the impact of incident recording and how this policy can be updated.

Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately using the log of concern form to the designated person for child protection, the Head Teacher. It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator. In the case of parents we will refer to child protection procedures.

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented using the child protection incident logging form (see appendix)

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your Human Resources (HR) and /or Teaching Union and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the Academy will follow the agreed procedures for dealing with any allegation against a member of staff and contact the Education Officer (see appendix).

Terms used in this policy

AUP: Acceptable Use Policy.

A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday. We use the term young person who is age 12 or over.

E-safety: We use e-safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children or Young people may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care. All staff have received training in 'Keeping safe in education'.

Schools: We refer specifically to Horizons Education Trust and special schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

Appendices/Cross references:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff from LSCB.
- Behaviour policy
- Safeguarding and Child Protection
- Keeping Children Safe in Education
- SRE (Sex and Relationships Education)
- PSHE Policy
- Safer Working Practices
- Data Protection Guidance
- Cambridgeshire Local Authority guidance (e.g. Use of Digital Images, e-mail)
- AUPs- staff, pupil, parents
- Anti-Bullying Policy
- Academy Complaints Procedure
- LA Infrastructure guidance (E2BN)
- Cambridgeshire Progression in ICT Capability Materials
- Risk assessment log
- Incident Log
- Computing Policy
- Academy rules for staying safe on the internet

Policy agreed on: JUNE 2024

Signed on behalf of the Trustees KIM TAYLOR

Committee: _____

Author: KIM TAYLOR

Review date (optional): JUNE 2026

Website Y/N