Online Safety Policy

The Eastwood Academy

Believe, Succeed, Together

Date Reviewed	June 2022
Date Ratified by Governing Body	July 2022

Contents

1.0 Introduction

ICT in the 21st century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Internet.
- Remote learning platforms.
- E-mail.
- Instant messaging often using simple web cams.
- Blogs.
- Podcasting.
- Social networking sites.
- Video broadcasting sites.
- Chat Rooms.
- Gaming Sites.
- Music download sites.
- Mobile/smart phones with text, video and web functionality.

In terms of online safety content, the risks can be broken down into the 4Cs:

- **Content** (being exposed to illegal or harmful content – e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism).
- **Contact** (being subjected to harmful online interaction with other users e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes).
- **Conduct** (online behaviour that increases the likelihood of, or causes, harm e.g. making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- **Commerce** (risks such as online gambling, inappropriate advertising, phishing and or financial scams. If pupils, or staff are at risk, this should be reported to the Anti-Phishing Working Group (APWG | Unifying The Global Response To Cybercrime)).

2.0 Online Safety

Online safety is a school's ability to protect and educate pupils and staff in their use of technology as well as having appropriate mechanisms in place to intervene and support any incident where appropriate. In short, the basis of an effective online safety policy is a thorough consideration of the 4Cs.

3.0 Responsibilities

3.1 Trust

The Trust has overall responsibility for online safety within its constituent academies which it delegates to Local Governing Bodies (LGB) and Principals. UK Council for Internet Safety - Governing Board Questions

3.2 Senior Leader

Vice Principal, Mr. C. Niner, has designated responsibility for online safety and is a CEOP Ambassador.

3.3 Staff

Broad responsibilities for teaching and support staff include:

- Taking responsibility for the security of Academy systems and data – refer to the Code of Conduct Policy.
- Having an awareness of online safety issues and how they relate to children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and take appropriate action by working with the Designated Safeguarding Lead (DSL) – refer to the Safeguarding Policy.
- Knowing when and how to escalate online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site – refer to Code of Conduct policy.
- Taking personal responsibility for professional development in this area.

Additional responsibilities for staff managing the technical environment include:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the SLT.
- Ensuring that suitable access controls and authentication/encryption is implemented to protect personal and sensitive information held on Academy-owned devices.
- Ensuring that the Academy's filtering* devices are updated and 'tested' on a regular basis.
- Ensuring that the use of the Academy's network is regularly monitored in order that any deliberate or accidental misuse can be reported.
- Reporting any breaches or concerns to the Senior Leadership Team (SLT) and DSL and applying appropriate action as advised.
- Developing an understanding of the relevant legislation which relates to the security and safety of the technical infrastructure.
- Reporting any breaches and liaising with the Local authority (LA) (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the Academy's ICT infrastructure/system is secure and not open to misuse or malicious attack.

- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensuring that appropriately strong passwords are applied and enforced.

**Filtering (at source) is provided by the service provider (Local Authority). In addition, the Academy has filtering software in place called Sophos XG and Sophos Central which locks down the desktops/laptops so that they cannot be modified or tampered with. This is monitored and policies have been created with restrictions managed in the cloud.*

The Academy uses Sophos XG to create rules which are used to only allow access to the internal network form the outside world. There are contrasting rulesets for pupils and staff to allow for a more flexible approach and age differentiation. A report is produced on a weekly basis and random checks are made regarding the nature of the sites accessed by staff and pupils. Sites are blocked when either monitoring and/or detection indicate their inappropriateness - UK Safer Internet Centre: Appropriate Filtering and Monitoring

3.4 Pupils

Responsibilities for pupils include:

- Adhering to the Academy's Acceptable Use Policy.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.

4.0 Education and Awareness

4.1 Information

The Academy's website has an individual online safety section for both parents and pupils:

Parents: http://www.eastwoodacademy.co.uk/index.php/parent/e-safety-for-parents
Pupils: http://www.eastwoodacademy.co.uk/index.php/pupils/e-safety-for-pupils

The following information will help parents keep their children safe online:

- Support for Parents to Keep Children Safe from Online Harm, which provides extensive resources to help keep children safe online and details of specific online risks, including sexual abuse, criminal exploitation and radicalisation.
- Support to Stay Safe Online, includes advice on security and privacy settings, content blocking and parental controls.

Additional resources to support parents to keep their children safe online include:

- Thinkuknow provides advice from the National Crime Agency (NCA) to stay safe online.
- Parent Info is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations.
- Childnet provides a tool kit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
- Internet Matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices and a host of practical tips to help children get the most out of their digital world
- LGfL provides support for parents and carers to keep their children safe online, including 6 top tips to keep primary aged children safe online.
- Net Aware provides support for parents and carers from the NSPCC, providing a guide to social networks, apps and games.
- Let's Talk About It provides support for parents and carers to keep children safe from online radicalisation.
- UK Safer Internet Centre provides tips, advice, guides and resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services.
- Staying safe online provides Government guidance offering advice on parental controls, fact-checking information, communicating with family and friends while social distancing is in place and taking regular breaks.
- NSPCC has advice on setting up parental controls, tips on how to talk to children about online safety, including the risk of sharing and receiving nude images and how to support children if they have seen something online that has upset them.
- Stop It Now resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour.
- Common Sense Media provides independent reviews, age ratings, & other information about all types of media for children and their parents

4.2 Delivery

Online safety awareness is delivered through the PDE curriculum, assemblies, external workshops and drop-down events.

4.3 Staff Training

All staff receive annual training in respect to the Data Protection Policy and ICT Acceptable Use Policy.

5.0 Data Protection

Refer to the Data Protection Policy.

6.0 ICT Acceptable Use

6.1 Staff

Refer to the Code of Conduct Policy.

6.2 Pupils

The policy is conveyed to parents and pupils principally in the Pupil Planner but also through assemblies and at relevant points in the curriculum.

In relation to the Academy computer network, and associated school-based ICT resources, I agree to adhere to the following:

- *Only use the computer network for school purposes.*
- *Never interfere with or damage the school computer network in any way. If I witness any misuse of the school computer network, I will report it to a member of staff.*
- *Only log on to the school network or learning platform using my own username and password.*
- *Regularly change my password and not reveal it to other pupils.*
- *Only use my school e-mail address.*
- *Never attempt to bypass the internet filtering system.*
- *Never knowingly access any material that could be considered inappropriate, offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.*
- *Ensure that my online activity, both inside and outside school, does not cause the Academy, staff, pupils or others distress or bring the reputation of the Academy into disrepute.*
- *Report to a member of staff or a parent any communication online or any material that makes me feel uncomfortable or asks me for personal information that I do not want to provide.*
- *Never reveal personal information including names, addresses, phone numbers and photographs of myself or others.*
- *Understand that my use of the internet and other related technologies is monitored and logged.*
- *Respect the copyright nature of material that I may find online.*
- *Never use downloaded material unless it is properly sourced and referenced.*
- *Understand that these rules are designed to keep me safe and that if they are not followed, sanctions will be applied.*

6.3 Mobile Phones, Cameras and other Electronic Equipment

In the case of staff, refer to the Staff Code of Conduct Policy.

In the case of pupils, mobile phones and other unnecessary electronic equipment are not permitted – refer to the Behaviour and Discipline Policy.

6.4 Use of Cameras and Images

Refer to the Data Protection Policy.

7.0 Remote Learning

Refer to Remote Learning Policy and Remote Learning FAQ

8.0 Dealing with Misconduct

8.1 Staff

Refer to the Safeguarding Policy and Disciplinary Misconduct Policy.

8.2 Pupils

Refer to the Behaviour and Discipline Policy.

8.21 Online Bullying

Online bullying, along with all other forms of bullying, of any member of the Academy's community will not be tolerated.

In cases of online bullying, the Pastoral Lead (Head of House) will discuss the incident with the SLT Link and Designated Safeguarding Lead (DSL). In cases of suspected gross misconduct, the incident will be referred to the Principal.

If the Academy is unclear if a criminal offence has been committed, then the DSL will obtain advice immediately through Children's Social Care and/or the Police.

The Academy will undertake the following in response to issues relating cyberbullying:

- Issue sanctions in line with the Behaviour and Discipline Policy.
- Where appropriate, contact the Police.
- Where appropriate contact Children's Social Care.
- Where appropriate, contact the Internet Service Provider (ISP).

8.22 Sexting (Sharing Nudes or Semi-Nudes) and Indecent Images of Children

The Academy will:

- Work in accordance with the SET Procedures (Southend Essex and Thurrock Safeguarding and Child Protection Procedures) and guidance from the UK Council for Child Internet Safety - sexting in schools and colleges - responding to incidents and safeguarding young people.
- Inform Children's Social Care and the Police, as appropriate.
- Store any devices/information involved securely.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.

8.23 Radicalisation and Extremism

The Academy will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of pupils.

When concerns are noted by staff that a child may be at risk of radicalisation online, then the DSL will be informed immediately and action will be taken in line with the Academy's Safeguarding Policy.

9.0 Information and Support

- www.thinkuknow.co.uk
- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.childnet.com/cyberbullying-guidance
- www.pshe-association.org.uk
- http://educateagainsthate.com/
- www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation
- www.gov.uk/UKCCIS- external visitors and online safety