Online Safety Policy

Document provenance

This policy was approved by Trustees as follows –	
Committee: Personnel Committee	Date of Approval: July 2022
Executive Leadership Team (ELT) Owner: National Safeguarding Director	Date of Review: July 2024
Unless there are legislative or regulatory changes in the interim, this policy will be reviewed every two years. Should no substantive changes be required at that point, the policy will move to the next review cycle.	

Policy purpose and summary

This Policy outlines the Trust approach to ensuring that everyone can work safely online. It sets out individual responsibilities to ensure compliance with this Policy.

Summary of changes at last review:

- Addition of 2.4 in relation to the impact of technology meaning that abuse can take place concurrently online and in daily life. Emphasis on the whole school approach.
- Additional scenarios for DSL action around sharing of indecent images including nudes or semi-nudes (consensual or non-consensual) and sexual violence and harassment (peer on peer abuse)
- Linked policy: CP & Safeguarding policy.
- Linked policy: Behaviour, Anti Bullying & Exclusions policy – Based on KCSE 2021 reference to the link between behaviour policies and cyberbullying.
- Addition within 3.2 of the 4th 'C' of 'commerce' in line with KCSE 2021.
- Addition to title from 'Filtering' to 'Filtering & Monitoring.'
- Inclusion of 4.2.2 (effective monitoring system i.e., Smootwall).
- Update to 5.8.2 in relation to terminology of 'cybercrime' and reference to Cyber Choices and the National Cyber Security Centre.
- Addition within 5.3.1 to link with KCSE 2021 expectation for an annual review/risk assessment of online safety provision.
- Removal of Appendix 2 (COVID-19 addendum) – Addition of 5.11 in relation to the DfE's 'Providing remote education: guidance for schools.

Related policies or guidance[1]:

- Data Protection Policy for Staff
- IT Acceptable Use Policy
- Social Media Policy
- Acceptable Use of Mobile Phones Policy
- Pupil Behaviour Policy
- Child Protection & Safeguarding Policy

[1] https://www.e-act.org.uk/e-act-policies/

Online Safety Policy

1. Introduction and Purpose

1.1. E-ACT is committed to promoting the welfare and safety of our students in all of our academies when using digital and online technologies. E-ACT recognises the importance of the contribution it can make to protecting and supporting students across its academies in their use of these technologies.

1.2. This policy is designed to incorporate all aspects of child protection and safeguarding that may be affected by digital technology, mobile phone technology, as well as E-ACT's use of technology with its academies.

1.3. The organisation will refer to the most recent government, Department for Education (DfE) and Information Commissioners Office (ICO) guidance and documentation with regard to data protection, data storage and privacy compliance.

2. Scope

2.1. This policy applies to all E-ACT staff (including agency), pupils/students, parents/carers, Trustees, Ambassadors, and other volunteers.

2.2. This policy applies to any individual who is given access to E-ACT's digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the organisation).

2.3. E-ACT expects all academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the school site. This will include imposing rewards and sanctions for behaviour - as defined as regulation or student behaviour under the Education and Inspections Act 2006[5]. The 'In Loco Parentis' duty allows the academy to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

2.4. As identified by Keeping Children Safe in Education[2], this policy recognises that technology plays a significant role in children's lives and abuse can take place concurrently online and in daily life. Online safety must therefore be considered as part of a whole school approach.

2.5. The Online Safety Policy covers the use of:

- School based IT systems and cloud-based software;
- School based intranet and networking;
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites;
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing;
- School IT equipment off-site, for example staff laptops, digital cameras, mobile

[222] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

phones, tablets, dongles;

- Student and staff personal IT equipment when used in school and which makes use of school networking, file-serving, or Internet facilities;
- Tablets, mobile phones, devices, and laptops when used on the academy site.

[1] http://www.legislation.gov.uk/ukpga/2006/40/contents

3. Policy Statement

3.1. The definition of an online incident is:

"Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of the Academy and/or E-ACT. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages, or any other means."

3.2. The most likely areas of risk to students are:

- Exposure to illegal inappropriate or harmful material;
- Subject to harmful online interactions with other users;
- The individual's personal online risky behaviour that then leads to harm.
- Online 'commerce' (online gambling, inappropriate advertising, phishing, or financial scams)

3.3. E-ACT has a responsibility for ensuring that the resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

3.4. We seek to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability both during their time in their academy and also in their future in their chosen careers and workplaces.

3.5. Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will receive online safety education as soon as they start using digital technology and this will be continually reinforced and monitored as students' progress through their school life.

3.6. E-ACT actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students, staff and the trust and associated academies and their reputations. We seek to promote a 'cyber aware' culture that ensures all staff, students and trustees take part in and continue to develop their knowledge and understanding of online behaviour and in particular, how to prevent harm through continual learning resources, research, and encouragement from all teachers.

4. Standards and Expectations

4.1. Systems

4.1.1. Academy computer systems will be configured to ensure the teaching and learning requirements of the academy are met whilst ensuring online safety is maintained.

4.1.2. Risk assessments are completed (a Data Privacy Impact Assessment, DPIA) when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

4.1.3. The system will be compliant with the academy, Trust, local authority, DfE, ICO and

Data Protection guidelines with regard to online safety procedures being met.

4.1.4. Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

4.1.5. Academy IT staff will be responsible for monitoring IT use.

4.2. Filtering & Monitoring

4.2.1. The academy will ensure an accredited filtering system is used. Filtering reports and logs will be examined regularly.

4.2.2. The academy will ensure an accredited monitoring system is used. Monitoring reports and logs will be examined regularly.

4.2.3. Any filtering incidents are examined, and action taken and recorded to prevent a recurrence. The academy will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

4.3. Network security

4.3.1. All users will have clearly defined access rights to academy technical systems and devices.

4.3.2. All users will be provided with a username and secure password by academy IT staff. Users are responsible for the security of their username and password.

4.3.3. The Network Manager and Headteacher/other designated senior person will have access to the main administrator password.

4.3.4. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.

4.4. Use of images and videos

4.4.1. The academy will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived, and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy (Appendix 1).

4.4.2. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the Internet e.g., social media sites.

4.4.3. Written permission from parents or from E-ACT will be obtained before photographs of students are published on the school website/social media/local press.

4.4.4. In accordance with guidance from the ICO, parents are able to take videos and digital

images of their children at academy events for their own personal use but should not be made publicly available where other students are involved in the digital imageor video.

4.4.5. Students must not take, use, share, publish or distribute images of others without their permission.

4.5. Data Protection

4.5.1. Personal data will be recorded, processed, transferred, and made available according to the Trust Data Protection Policy and in compliance with GDPR and the Data Protection Act (1998).

4.6. Social Media

4.6.1. Trustees, academy, national and regional team staff, students and volunteers are expected to comply with the Trust's Social Media Policy.

5. Responsibilities

5.1. Headteachers should ensure that all academy staff and visitors are aware of the Online Safety Policy and procedure and of their responsibilities set out in this policy. It is the responsibility of the Headteacher to ensure that breaches of the policy are investigated and addressed.

5.2. Academy staff, regional and national team staff, ambassadors and trustees are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

5.3. Academy management and online safety

5.3.1. Academy Senior Leadership Teams (SLTs) are responsible for determining, evaluating and reviewing online safety to encompass teaching and learning, use of academy IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, school staff and trustees of Internet capable equipment for academy related purposes, or in situations which will impact on the reputation of the academy, and/or on academy premises. This is in line with expectations in Keeping Children Safe in Education in relation to an annual review/risk assessment of online safety provision.

5.3.2. Regular assessment of the strengths and weaknesses of practice within the academy will help determine INSET provision needed for staff and guidance provided to parents, students, and local partnerships.

5.4. Online Safety Co-ordinator

5.4.1. The academy has a designated Online Safety Co-ordinator (see individual academy website for contact details) who reports to the Senior Leadership Team and co-ordinates online safety provision across the academy and wider school community.

5.4.2. The academy's Online Safety Co-ordinator is responsible for online safety issues on a day to day basis and also liaises with relevant stakeholders including IT support, the Trust's Regional Safeguarding System Leader, and other Trust contacts, to ensure the safety of students.

5.4.3. The Online Safety Co-ordinator maintains a log of submitted online safety reports and incidents.

5.4.4. The Online Safety Co-ordinator audits and assesses inset requirements for staff, support staff and trustee online safety training, and ensures that all staff are aware of their responsibilities and the academy's online safety procedures. The Co-ordinator is also the first port of call for staff requiring advice on online safety matters.

5.4.5. The Online Safety Co-ordinator is responsible for promoting best practice in online safety within the wider academy community, including providing and being a source of information for parents and partner stakeholders. This may include facilitating regular assemblies and other such activities that focus on positive messages and behaviours.

5.4.6. The Online Safety Co-ordinator will be involved in any risk assessment of new technologies, services, or software to analyse any potential risks.

5.5. Trustees and regional team

5.5.1. The Trustees delegate a number of functions to the national and regional teams. The Regional Safeguarding System Leader, on behalf of the Board of Trustees, and the academy's Online Safety Co-ordinator will liaise directly with one another with regard to reporting on online effectiveness, incidents, monitoring, evaluation to the Executive Leadership Team (ELT) and the Education Committee, and developing and maintaining links with local stakeholders and wider academy community.

5.5.2. This is important also to provide and evidence of a link between the academy, trustees, and parents.

5.5.3. Regional Safeguarding System Leaders must ensure that they have demonstrable experience, skills and training to be able to provide appropriate challenges and support to the academy management team.

5.6. IT support staff

5.6.1. Internal IT support staff are responsible for maintaining the academy's networking, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the academy system, particularly file-sharing and access to the Internet, is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.

5.6.2. IT support staff in academies are responsible for:

- Defending the network and infrastructure of the academy, reviewing activity logs regularly;
- Ensuring that users comply with basic access policies and that only trusted devices can connect to the academy network;
- Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised;

- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team and Online Safety Co-ordinator;
- To report to the management team and Online Safety Co-ordinator on any network intrusions or other threats to the network;
- To ensure that any IT outsourced e.g., connectivity, maintenance, cloud-based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations;
- Promoting basic cyber security practices within the academy e.g., locking computers when away from the desk, using secure passwords, caution when using USB removable drives.

5.6.3. External contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.

5.7. All Staff

5.7.1. Teaching and support staff are responsible for ensuring that they understand the Trust's Online Safety Policy, practices, and associated procedures for reporting online safety incidents in line with academy procedures.

5.7.2. All staff will be provided with an online safety induction as part of the overall staff induction procedures. All staff will attend mandatory online safety training provided by the academy or the Regional Safeguarding System Leader.

5.7.3. All staff will ensure that they have read, understood, and signed the Acceptable Use Policy (Appendix 1) relevant to Internet and computer use in each academy.

5.7.4. All teaching staff are to be vigilant in monitoring student Internet and computer usage in line with the policy. This may include the use of personal technology, such as cameras and phones on the school site where there is a cause for concern.

5.7.5. Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

5.7.6. Staff must promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.

5.7.7. Staff must report as soon as is practicable any suspected misuse of Trust/academy digitally connected systems to the Headteacher or Online Safety Co-ordinator.

5.8. Designated Safeguarding Lead (DSL)

5.8.1. The DSL will be trained in specific online safety issues e.g., CEOP accredited course or equivalent.

5.8.2. The DSL will be responsible for escalating online safety incidents to the relevant external parties e.g., CEOP, Cyber Choices, National Cyber Security Centre, local Police, Local Safeguarding Children's Board, social care and parents/E-ACTs, ELT. Possible scenarios might include:

- Allegations against members of staff;
- Cybercrime – illegal hacking, denial of service, use of malware;
- Allegations or evidence of 'grooming;'
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment, or a malicious communication;
- Sharing of indecent images including nudes or semi-nudes (consensual or non-consensual) [OBJ];
- Sexual violence or harassment between peers (peer on peer abuse).

5.8.3. The DSL is responsible for acting 'in loco parentis' and liaising with websites and social media platforms, such as Twitter and Facebook, to remove instances of illegal material or cyber bullying.

5.9. Pupils/Students

5.9.1. Pupils/students must ensure use of academy Internet and computer systems in agreement with the terms specified in the policy. In secondary phases, students are expected to sign the policy to indicate agreement.

5.9.2. Students are responsible for ensuring they report online safety incidents in the academy or with other external reporting facilities, such as CEOP or Childline, and are expected:

- To be aware of and comply with academy policies for Internet and mobile technology usage in the academy, including the use of personal items such as mobile phones;
- To be aware that their Internet use out of the academy on social networking sites, is covered under the Online Safety Policy if it impacts on the academy and/or its staff and students in terms of cyber bullying, reputation, or illegal activities;
- To follow basic cyber security practices within the academy e.g., locking computers when away from the desk, using secure passwords, caution with use of USB removable drives.

5.10. Parents/Carers

5.10.1. Parents/carers must support the academy in its promotion of good Internet behaviour and responsible use of IT equipment and mobile technologies both at the academy and at home.

5.10.2. Where appropriate, parents should sign the academy's Acceptable Use Policy (Appendix 1), indicating agreement regarding their child's user and also their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangements and questionnaires.

5.11 Remote Education

5.11.1. Academies will have due regard to the DfE's 'Providing remote education: guidance for schools[3]' after the expiration of the temporary provisions in the Coronavirus Act

[3] https://www.gov.uk/government/publications/providing-remote-education-guidance-for-schools

2020 in relation to remote education.

6 Review

6.10 This policy will be monitored as part of the academy's annual internal review and reviewed on a two-year cycle or as required by legislation changes.

6.11 An up-to-date copy of the policy will be available on the E-ACT website.

Appendix 1: Example wording for Acceptable Use Policy

Exemplar wording for an Acceptable Internet Use Statement for Students and Staff

In , students and teachers work in partnership within a learning community. Mutual respect, responsible attitudes to each other, to work and to property are at the foundation of each Academy's culture of achievement by all.

The computer systems at all E-ACT academies are the property of that academy and are a resource shared by all students and staff. Computer facilities, including portable units, are made available to students to further their education and to staff to enhance their professional activities, including teaching, research, administration, and management. Each Academy's Internet Access Policy has been drawn up to protect all parties - the students, the staff, and the Academy. Please contact the Headteacher for a copy of the Academy's Internet Acceptable Use Policy.

Key Points:

The Academy reserves the right to examine or delete any files, including emails, that may be held on its computer system and to monitor or restrict access to any Internet sites visited.

Students and staff using the Academy's computer system should sign a copy of this Acceptable Internet Use Statement and return it to:

- General Office in respect of Students.
- Headteacher's Office in respect of Staff (to remain on personnel file)
- All Internet activity should be appropriate to staff professional activity, student's education, or reasonable social use;
- Access to the Internet should only be made via the user's authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the Academy ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all email sent and for contacts made that may result in email being received;
- Copyright of materials must be respected;
- Use of personal financial gain, gambling or political purposes is forbidden;
- Use of the network to access inappropriate material is forbidden.

Name / Tutor Group or Class / Department.

Signed Student / Parent / Staff / Date

REMOTE WORKING - KEEPING IT SAFE

Working from home and accessing personal data from outside of the academy presents us with a new set of risks that we all need to be aware of and think about in order to keep staff & students and their data safe.

Use of school devices for school work.

If you have been given a school device, you should use this at all times when accessing school data and websites. This device should have appropriate controls and safeguards in place to ensure that data is kept secure.

School devices are for school employees only and should not be used by any other members of the family or household.

Use of personal devices for school work

When accessing school emails and resources on a non-school provided device, staff are reminded that personal data should not be downloaded or saved to such devices.

Staff should use online web apps such as Microsoft Office 365 and edit work/emails in the cloud. You can access these using the office 365 portal.

Be aware of Phishing Emails

Unfortunately, at times like this there are still people who are looking to take advantage of the situation.
Please pay particular attention to emails that could be phishing

- Senders email address doesn't match the organisations address
- Spelling / grammatic mistakes
- Urgency in requests for action
- Requests to input personal credentials

Microsoft Teams

Microsoft Teams is a great way to keep in touch and hold meetings.

If you are using the video function

- Dress appropriately,
- Be mindful of what's in the background – use the blur background function
- It is not recommended to have 1:1 video and team meetings with students

Use secure passwords and keep them safe

Make sure they are not accessible by others. Lock your device when not in use.

Removeable Media

Do not save any personal data onto removeable media (USB drives, CD's etc). Use approved tools and services already provided by the trust.

You can save files and resources to One drive through the Office 365 portal.

https://portal.office.com

Use official communication channels

Remember to only use official communication channels when communicating personal information about staff & students such as school email and Microsoft Teams.

Stay Alert & Report if unsure

If something looks or seems not right it probably isn't. Your IT Teams are working throughout this whole period and would rather get lots of false alerts than not being alerted to something that's wrong.

For help or more information please contact your local IT support in the usual way