EASTERN MULTI-ACADEMY TRUST

Group Policy Document

E SAFETY POLICY

Summary

This policy document is to detail the procedures to safeguard and support staff and learners to identify and manage risks associated with digital technologies at all Eastern Multi-Academy Trust settings.

If you are unsure about the validity of the content of this policy please refer to the Policy Owner.

Please Note: This policy is applicable to All Employees / Teachers / Support Staff / Volunteers including Trustees and Governors within the Group.

Policy owner	**Audit Committee**
Policy holder	**Chief Executive Officer**
Author	David Cousins, Chief Finance Officer Rebecca Schrooder, Operations Manager

Policy Inventory ID Number	**DP03**
Group Policy Area	IT Security and GDPR Policies

Approved by

Consultation Group	**Audit Committee**
Approval Committee	**Audit Committee**
Implementation date	**July 2025**
Review Date	**July 2028**

Version Control

Control No	Change summary	Consultation Group	Effective date
01	Reviewed with no changes	ELT Audit	July 2025

Eastern Multi-Academy Trust (referred to as The Trust) recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within the Trust and to support staff and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies.

In furtherance of our duty to safeguard learners, including meeting the new PREVENT requirements, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

This e-safety policy should be read in conjunction with other relevant Trust policies and procedures.

The policy applies to all users who have access to the Trust IT systems, both on the premises and remotely, and to all use of the internet and electronic communication devices such as email, mobile phones, games consoles, social networking sites, etc.

OBJECTIVES OF THE POLICY

1. Safeguards on Trust IT-based systems are strong and reliable.
2. Behaviour of users of systems is safe and appropriate.
3. Storage and use of images and personal information on Trust IT- based systems is secure and meets all legal requirements.
4. Staff and students are well educated in e-safety.
5. Any incidents which threaten e-safety are well managed.
6. Students understand the risks attached to accessing terrorist and extremist material online and understand the institution's duty and process in these areas.

INTENDED OUTCOMES

1. Security

1.1 Trust networks are safe and secure insofar as possible, with appropriate and up to-date security measures and software in place.
1.2 Digital communications, including email and internet postings, over the Trust network, are monitored as far as is practicable.

2. Risk assessment

2.1 When making use of new technologies and online platforms, risk assessments are carried out.

3. Behaviour

3.1 All users of technology adhere to the standards of behaviour set out in the Trust's IT Acceptable use policies.
3.2 All users of IT adhere to Trust guidelines when on email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras, etc.
3.3 Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) online are dealt with seriously, in line with staff and student disciplinary procedures.
3.4 Any conduct considered illegal or extreme is reported to the police or appropriate authorities.

4. Use of images and video

4.1 The use of images or photographs is encouraged in teaching and learning.
4.2 There is no breach of copyright or other rights of another person.
4.3 Staff and students are trained in the risks in downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example.
4.4 Staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe.
4.5 Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any image.
4.6 Published photographs do not include names of individuals.
4.7 Consent is sought for the use of images or video of both students and staff, as appropriate.

5. Personal information

5.1 Processing of personal information is done in compliance with General Data Protection Regulations (GDPR) and the Data Protection Act.
5.2 Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
5.3 No personal information is posted to the Trust website/intranets without the permission of a senior manager and the express permission of the individual.
5.4 Staff keep learners' personal information safe and secure at all times.
5.5 All personal information is password protected.
5.6 No personal information of individuals is taken offsite unless the member of staff has the permission of their manager.
5.7 Every user of IT facilities logs off on completion of any activity, or locks the machine or ensures rooms are locked if unsupervised, where they are physically absent from a device or when accessing

web based services remotely.
5.8 Documents with sensitive data are password protected
5.9 Personal data no longer required, is securely deleted.

6. Education and Training

6.1 Staff and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.
6.2 Learner induction and the programme of pastoral tutorials contain sessions on e-safety and the need for students and staff to be aware of the consequences of inappropriate use of IT systems and specific websites.
6.3 Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.
6.4 Learners know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.
6.5 In classes, learners are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.
6.6 Staff are e-safety trained. Further resources of useful guidance and information are issued to all staff as available.
6.7 Any new or temporary users receive basic training on the Trust IT system.

7. Incidents and response

7.1 A clear and effective incident reporting procedure is maintained and communicated to students and staff.
7.2 Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.
7.3 Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (eg the police), review of internal procedures and safeguards, pastoral support for affected students, etc.
7.4 Any breaches of this policy should be reported in the first instance to the Trust Chief Executive or Academy Principal

RESPONSIBILITIES

- The **Chief Finance Officer** is responsible for maintaining this policy, and the following are responsible for implementing it.
- **The Trust's Data Protection Officer, Chief Finance Officer and Director of People** is responsible for investigating reported breaches and for all e- safety matters in relation to Trust staff. In addition, these posts are responsible for maintaining best practice in IT procedures and practices to manage any e-safety risks effectively.
- **The Principals of each Academy** are responsible for incorporating e-safety in student induction and the pastoral tutorial framework.
- **Teachers** are responsible for delivering an appropriate programme of education and for embedding e safety education and practice into their teaching programme.
- **The Principals of each Academy** are responsible for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.