East Midlands
Academy Trust

East Midlands Academy Trust

Online Safety Policy 2023/2025

‘Every child deserves to be the best they can be’

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V4	**Filename:** EMAT Online Safety Policy
Approval: Sept 2023 *Approved by the Trust Board*	**Next Review: Sept 2025** *This Policy will be reviewed by the Trust Board (FHRE committee) every two years*
Owner: East Midlands Academy Trust Board of Trustees	**Union Status:** Not Applicable

Policy type:	
Non-Statutory	Replaces Academy's current policy

Revision History

RevisionDate	Revisor	Description of Revision
Sept 2023 - v4	DU / Thompson Team	Updated to additional information reflecting updates to KCSIE and to align with changes made in the Safeguarding and Child Protection Policy.
February 2022	DU	Policy update – no changes
April 2023	DU	Minor changes & addition of required "NCSC Cyber Security Training for School Staff" for all staff, Trustees and LAB members
June 2023	DU	Updated to reflect KCSIE Update for September 2023

Contents

EMAT Online Safety Policy

1. Aims

East Midlands Academy Trust (EMAT) aims to:

- ✓ Have robust processes in place to ensure the online safety of learners, staff, volunteers, trustees, members and Local Advisory Board (LAB) members;
- ✓ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- ✓ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as 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, such as 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; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, 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

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996, 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 learners' electronic devices where they believe there is a 'good reason' to do so.

The policy complies with EMAT'S funding agreement and articles of association.

3. Roles and Responsibilities:

Roles and responsibilities are outlined in Appendix ? when referring to the DfE filtering and monitoring standards and DfE cyber security standards.

3.1. The Trustees

The board of Trustees has overall responsibility for monitoring this policy and holding the CEO to account for its implementation. The Audit and Risk Committee of Trustees will review the policy on a two-year cycle or as required by legislation changes.

All Trustees will:

- Ensure EMAT has appropriate filtering and monitoring systems in place and regularly review their effectiveness.
- Ensure the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively.
- Ensure that the leadership team and relevant staff know how to escalate concerns when identified.
- Consider the number of and age range of their children in the school, those who are potentially at greater risk of harm and how often they access the IT system.
- Review the standards (filtering and monitoring) and liaise with IT staff what more needs to be done to support school in meeting this standard
- Ensure that all staff undergo online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Ensure that 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 (appendix 1).

3.2. Local Advisory Board (LAB) Members

The LAB Members for each academy are responsible for holding the headteacher to account for this policies implementation. LAB Members will:

- Ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness.
- Ensure the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively.
- Ensure that the leadership team and relevant staff know how to escalate concerns when identified
- Consider the number of and age range of their children in the school, those who are potentially at greater risk of harm and how often they access the IT system.
- Ensure that all staff undergo online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

- Co-ordinate termly meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school 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).

All LAB Members will:

- Ensure that 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 (appendix 1)

3.3. The Head Teacher

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. They will:

- Ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness.
- Ensure the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively.
- Ensure that the leadership team and relevant staff know how to escalate concerns when identified.
- Oversee filtering and monitoring reports.
- Make sure that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
- Consider the number of and age range of their children in the school, those who are potentially at greater risk of harm and how often they access the IT system.

3.4. The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) [and deputy DSL] are set out in our child protection and safeguarding policy as well as relevant job descriptions. 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, IT Business Partner and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on My Concern and dealt with

appropriately in line with the school relational behaviour policy.

- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing termly reports on online safety in school to the headteacher and LAB Members.
- Understanding the filtering and monitoring systems and processes in place.
- Reviewing filtering and monitoring reports to identify safeguarding concerns.
- Carry out checks to filtering and monitoring systems.

All DSLs and Deputy DSLs will:

- Ensure that 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 (appendix 1).

3.5. IT Business Partner

The IT Business Partner is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners 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 on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents recorded using IT system are sent to the relevant DSL for each school automatically.
- Ensuring that any incidents of cyber-bullying identified with IT Systems are sent to the relevant DSL as each school automatically.
- Ensuring that the ICT Infrastructure for EMAT is in line with the DfE's Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

3.6. All staff

All staff are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Ensuring that learners follow the school's terms as outlined in the Learner ICT Acceptable Use Policy (APU), Appendix 1.
- Working with the DSL to ensure that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with EMAT'S Behaviour Policy.
- Reporting all reports and concerns about sexual violence and/or harassment to the DSL, both online and offline and maintaining an attitude of 'it could happen here'.
- Understanding the expectations and their roles and responsibilities in relation to filtering and monitoring processes in place.

All staff will:

- Ensure that 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 (appendix 1).

3.7. Parents / Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- In primary phase academies they should ensure their child has read, understood and agreed to the terms on EMATs Acceptable Policy (Appendix 1).

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites: UK Safer Internet Centre , Childnet International

3.8. Visitors and members of the community

Visitors and members of the community who use EMAT's ICT Infrastructure will be made aware of this policy, when relevant, and expected to read and follow it.

4.0. Educating Learners

EMAT aims to develop learners as digital citizens. Learners will be taught about online safety as part of the curriculum. It is also taken from the Guidance on relationships education, relationships and sex education (RSE) and health education.

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

4.1. Key Stage 1

Learners 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.

4.2. Key Stage 2

Learners 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.

4.3. End of Primary

By the end of primary school, learners will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

4.4. Key Stage 3

Learners 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.

4.5 Key Stage 4

Learners 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.

4.6 End of secondary

By the end of secondary school learners will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and

negatively affect how they behave towards sexual partners.

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

The safe use of social media and the internet will also be covered in other subjects where relevant.

4.7 SEND Provision

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

EMAT's academies will raise parents'/carers' awareness of internet safety using Arbor Parent Portal or other communications home, in information via our website, social media and in school activities. This policy will also be shared with parents/carers via school website. If parents/carers 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.

6. Cyber-bullying

6.1 Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

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

The EMAT schools will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their class/tutor groups, and the issue will be addressed in assemblies.

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. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school 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 contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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 learners' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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;
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. Staff will not delete any material. If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

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

7. Acceptable Usage

All pupils, parents/carers, staff, volunteers and LAB Members and Trustees are expected to sign an agreement regarding the acceptable use of EMATs ICT systems and infrastructure (appendix 1).

Visitors will be expected to read and agree to the Acceptable Usage policy if relevant.

Use of EMAT's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. EMAT monitors (via CISCO Firewalls and the app 'SENSO' the websites visited by pupils, staff, volunteers, LAB members, trustees and visitors (where relevant) to ensure they comply with the above.

8. Learners using mobile devices in school

8.1 Learners in the Primary Phase

Learners in Primary Phase may, at the discretion of the schools Headteacher bring mobile devices into school which are then handed in to a staff member for the duration of the school day. Pupils are not permitted to bring in or use devices such as Smart watches, which have a camera, internet connectivity and/or mobile technology (can be used for messages and calls).

8.2 Learners in Secondary Phase

Learners in the secondary phase may bring mobile devices into school but are not permitted to use them during the school day. All phones are turned off before entering the school grounds and they are not to be used until they have left site. Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

8.3 Learners in the 6th form

Learners in the 6th form can bring devices on site and use these in the designated 6th Form areas for the purpose of research and study, but not outside this area, e.g. in corridors etc. This is to ensure we maintain the ethos and rules of the rest of the school. Phones should be switched off when moving around the building and attending lessons. 6th Form Learners should sign the 'Bring Your Own Device Agreement' should they wish to use their devices in this way.

9. Staff using work devices offsite

Staff members using a work device offsite must comply with the following:

- Not install or attempt to install any unauthorised software on the device.
- Not use the device in any way which would violate EMAT's Acceptable Usage policy (see appendix 1).
- Do not share their password with others (see appendix 1 for exceptions).
- Must take all reasonable steps to ensure the security of their work device when using it outside school.
- Must not let other unauthorised person use their work device including friends and family.
- Report any concerns over the security of their device to the IT Service Desk.

10. How EMAT will respond to issues of misuse

Where a pupil misuses EMAT's ICT systems or internet, the relevant school will follow the procedures set out in relevant behaviour policy and or EMAT's Acceptable Usage Policy.

Where a staff member misuses EMAT IT Systems and infrastructure, or misuses a device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and or Acceptable Usage Policy by EMAT's HR Department.

Any illegal activity or content, they will be reported to the police.

11. Training

All staff members will undertake NCSC Cyber Security Training for School Staff training and will be expected to retake the training every two years as part of the EMAT's mandated training.

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).

The DSL and deputies 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.

Trustees will undertake NCSC Cyber Security Training for School Staff training part of their required training.

All staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring at induction and updated regularly.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring

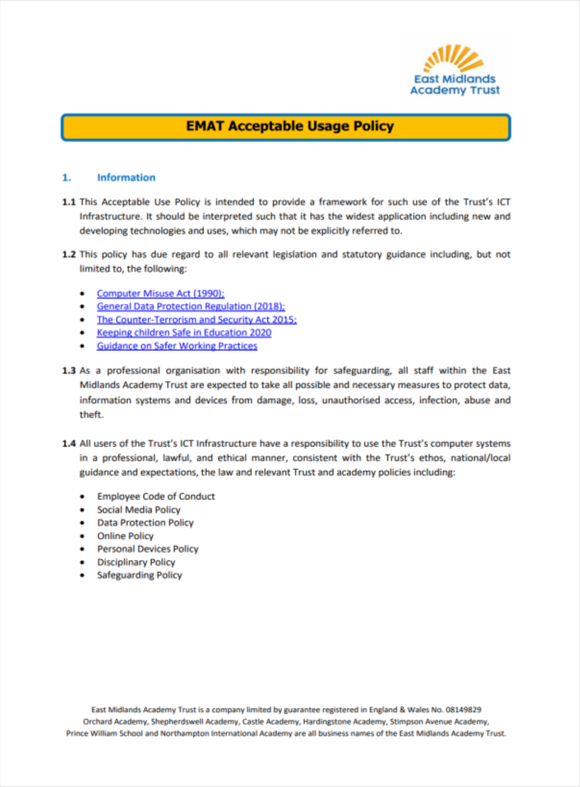
The DSL or deputy DSL for each school will log all safeguarding issues related to online safety. This information is held on My Concern. This policy will be reviewed every year by the Designated Safeguarding Lead and or Deputy Designated Lead and Headteachers. At every review, the policy will be shared with the appropriate LAB Members.

13. Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and Child Protection Policy
- Dealing with allegations of abuse against staff members
- Staff Code of conduct
- Anti-bullying policy and procedures
- Acceptable Usage Policy
- Behaviour Policy

Appendix 1 – Acceptable Usage Policy



EMAT Acceptable Usage Policy

1. Information

1.1 This Acceptable Use Policy is intended to provide a framework for such use of the Trust's ICT Infrastructure. It should be interpreted such that it has the widest application including new and developing technologies and uses, which may not be explicitly referred to.

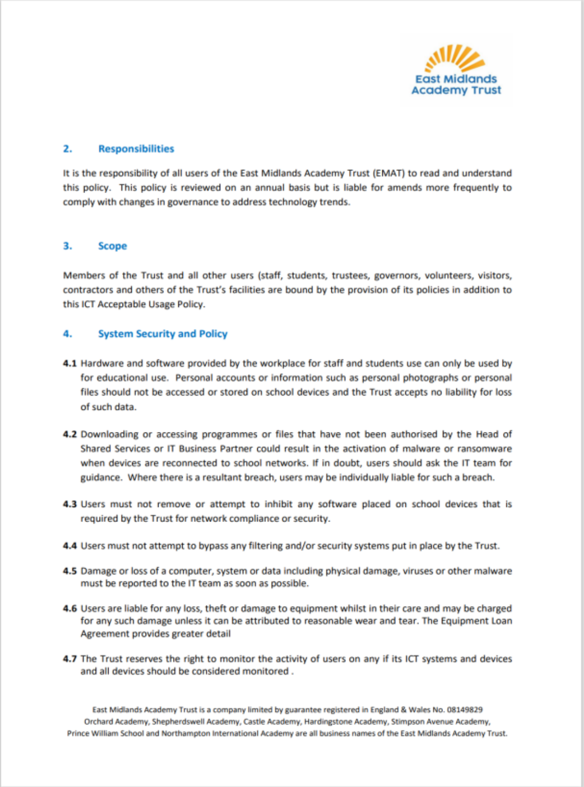
1.2 This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Computer Misuse Act (1990);
- General Data Protection Regulation (2018);
- The Counter-Terrorism and Security Act 2015;
- Keeping children Safe in Education 2020
- Guidance on Safer Working Practices

1.3 As a professional organisation with responsibility for safeguarding, all staff within the East Midlands Academy Trust are expected to take all possible and necessary measures to protect data, information systems and devices from damage, loss, unauthorised access, infection, abuse and theft.

1.4 All users of the Trust's ICT Infrastructure have a responsibility to use the Trust's computer systems in a professional, lawful, and ethical manner, consistent with the Trust's ethos, national/local guidance and expectations, the law and relevant Trust and academy policies including:

- Employee Code of Conduct
- Social Media Policy
- Data Protection Policy
- Online Policy
- Personal Devices Policy
- Disciplinary Policy
- Safeguarding Policy



2. Responsibilities

It is the responsibility of all users of the East Midlands Academy Trust (EMAT) to read and understand this policy. This policy is reviewed on an annual basis but is liable for amends more frequently to comply with changes in governance to address technology trends.

3. Scope

Members of the Trust and all other users (staff, students, trustees, governors, volunteers, visitors, contractors and others of the Trust's facilities are bound by the provision of its policies in addition to this ICT Acceptable Usage Policy.

4. System Security and Policy

4.1 Hardware and software provided by the workplace for staff and students use can only be used by for educational use. Personal accounts or information such as personal photographs or personal files should not be accessed or stored on school devices and the Trust accepts no liability for loss of such data.

4.2 Downloading or accessing programmes or files that have not been authorised by the Head of Shared Services or IT Business Partner could result in the activation of malware or ransomware when devices are reconnected to school networks. If in doubt, users should ask the IT team for guidance. Where there is a resultant breach, users may be individually liable for such a breach.

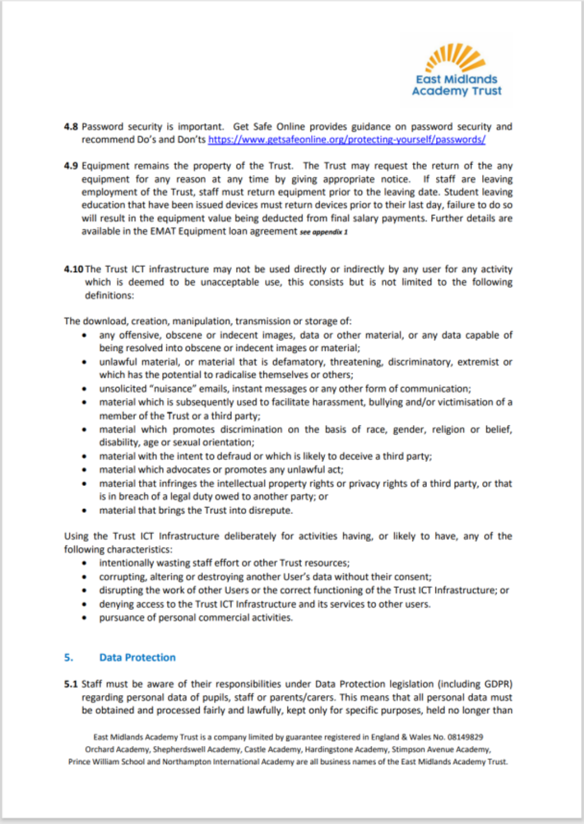
4.3 Users must not remove or attempt to inhibit any software placed on school devices that is required by the Trust for network compliance or security.

4.4 Users must not attempt to bypass any filtering and/or security systems put in place by the Trust.

4.5 Damage or loss of a computer, system or data including physical damage, viruses or other malware must be reported to the IT team as soon as possible.

4.6 Users are liable for any loss, theft or damage to equipment whilst in their care and may be charged for any such damage unless it can be attributed to reasonable wear and tear. The Equipment Loan Agreement provides greater detail

4.7 The Trust reserves the right to monitor the activity of users on any if its ICT systems and devices and all devices should be considered monitored .



4.8 Password security is important. Get Safe Online provides guidance on password security and recommend Do's and Don'ts https://www.getsafeonline.org/protecting-yourself/passwords/

4.9 Equipment remains the property of the Trust. The Trust may request the return of the any equipment for any reason at any time by giving appropriate notice. If staff are leaving employment of the Trust, staff must return equipment prior to the leaving date. Student leaving education that have been issued devices must return devices prior to their last day, failure to do so will result in the equipment value being deducted from final salary payments. Further details are available in the EMAT Equipment loan agreement ***see appendix 1***

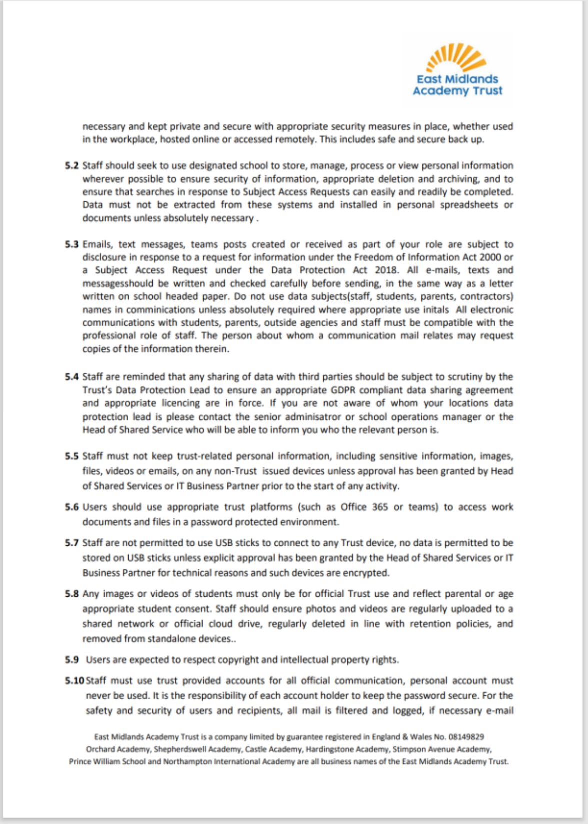
4.10 The Trust ICT infrastructure may not be used directly or indirectly by any user for any activity which is deemed to be unacceptable use, this consists but is not limited to the following definitions:

The download, creation, manipulation, transmission or storage of:
- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
- unsolicited "nuisance" emails, instant messages or any other form of communication;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Trust or a third party;
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
- material that brings the Trust into disrepute.

Using the Trust ICT Infrastructure deliberately for activities having, or likely to have, any of the following characteristics:
- intentionally wasting staff effort or other Trust resources;
- corrupting, altering or destroying another User's data without their consent;
- disrupting the work of other Users or the correct functioning of the Trust ICT Infrastructure; or
- denying access to the Trust ICT Infrastructure and its services to other users.
- pursuance of personal commercial activities.

5. Data Protection

5.1 Staff must be aware of their responsibilities under Data Protection legislation (including GDPR) regarding personal data of pupils, staff or parents/carers. This means that all personal data must be obtained and processed fairly and lawfully, kept only for specific purposes, held no longer than



necessary and kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. This includes safe and secure back up.

5.2 Staff should seek to use designated school to store, manage, process or view personal information wherever possible to ensure security of information, appropriate deletion and archiving, and to ensure that searches in response to Subject Access Requests can easily and readily be completed. Data must not be extracted from these systems and installed in personal spreadsheets or documents unless absolutely necessary .

5.3 Emails, text messages, teams posts created or received as part of your role are subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018. All e-mails, texts and messagesshould be written and checked carefully before sending, in the same way as a letter written on school headed paper. Do not use data subjects(staff, students, parents, contractors) names in comminications unless absolutely required where appropriate use initals All electronic communications with students, parents, outside agencies and staff must be compatible with the professional role of staff. The person about whom a communication mail relates may request copies of the information therein.

5.4 Staff are reminded that any sharing of data with third parties should be subject to scrutiny by the Trust's Data Protection Lead to ensure an appropriate GDPR compliant data sharing agreement and appropriate licencing are in force. If you are not aware of whom your locations data protection lead is please contact the senior adminisatror or school operations manager or the Head of Shared Service who will be able to inform you who the relevant person is.

5.5 Staff must not keep trust-related personal information, including sensitive information, images, files, videos or emails, on any non-Trust issued devices unless approval has been granted by Head of Shared Services or IT Business Partner prior to the start of any activity.

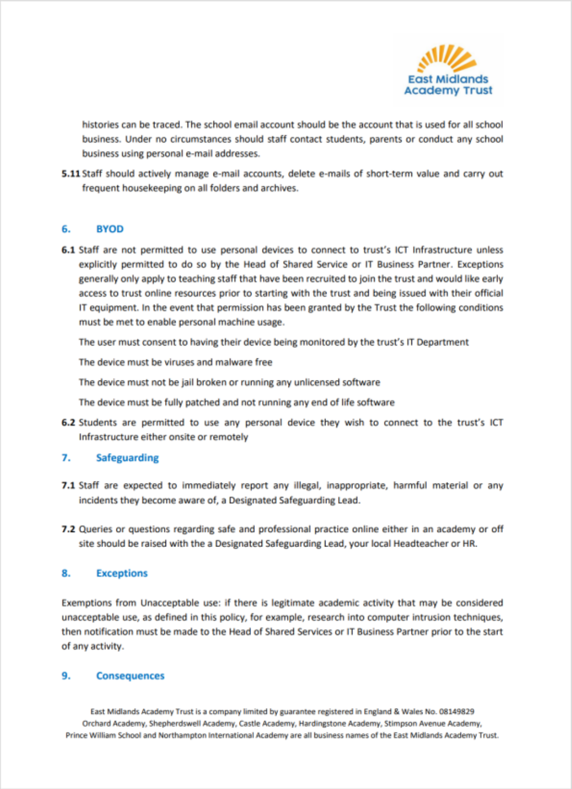
5.6 Users should use appropriate trust platforms (such as Office 365 or teams) to access work documents and files in a password protected environment.

5.7 Staff are not permitted to use USB sticks to connect to any Trust device, no data is permitted to be stored on USB sticks unless explicit approval has been granted by the Head of Shared Services or IT Business Partner for technical reasons and such devices are encrypted.

5.8 Any images or videos of students must only be for official Trust use and reflect parental or age appropriate student consent. Staff should ensure photos and videos are regularly uploaded to a shared network or official cloud drive, regularly deleted in line with retention policies, and removed from standalone devices..

5.9 Users are expected to respect copyright and intellectual property rights.

5.10 Staff must use trust provided accounts for all official communication, personal account must never be used. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged, if necessary e-mail



histories can be traced. The school email account should be the account that is used for all school business. Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.

5.11 Staff should actively manage e-mail accounts, delete e-mails of short-term value and carry out frequent housekeeping on all folders and archives.

6. BYOD

6.1 Staff are not permitted to use personal devices to connect to trust's ICT Infrastructure unless explicitly permitted to do so by the Head of Shared Service or IT Business Partner. Exceptions generally only apply to teaching staff that have been recruited to join the trust and would like early access to trust online resources prior to starting with the trust and being issued with their official IT equipment. In the event that permission has been granted by the Trust the following conditions must be met to enable personal machine usage.

The user must consent to having their device being monitored by the trust's IT Department

The device must be viruses and malware free

The device must not be jail broken or running any unlicensed software

The device must be fully patched and not running any end of life software

6.2 Students are permitted to use any personal device they wish to connect to the trust's ICT Infrastructure either onsite or remotely

7. Safeguarding

7.1 Staff are expected to immediately report any illegal, inappropriate, harmful material or any incidents they become aware of, a Designated Safeguarding Lead.

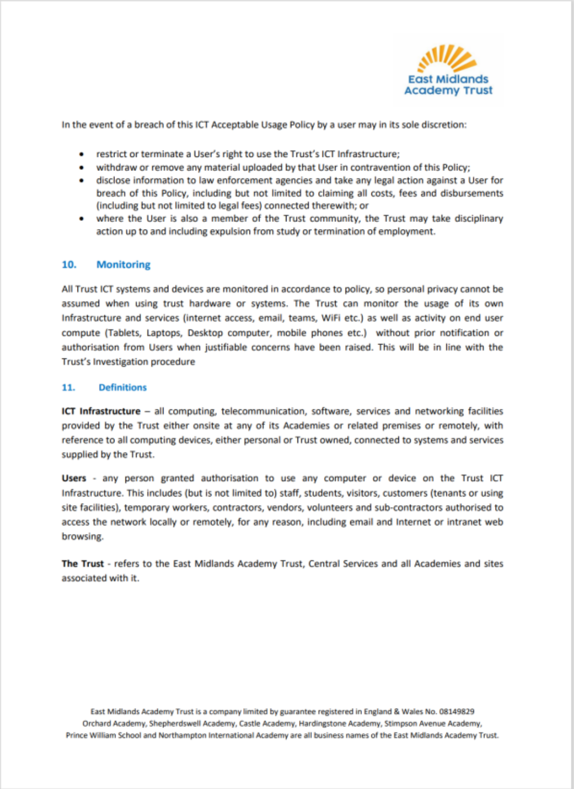
7.2 Queries or questions regarding safe and professional practice online either in an academy or off site should be raised with the a Designated Safeguarding Lead, your local Headteacher or HR.

8. Exceptions

Exemptions from Unacceptable use: if there is legitimate academic activity that may be considered unacceptable use, as defined in this policy, for example, research into computer intrusion techniques, then notification must be made to the Head of Shared Services or IT Business Partner prior to the start of any activity.

9. Consequences

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.



In the event of a breach of this ICT Acceptable Usage Policy by a user may in its sole discretion:

- restrict or terminate a User's right to use the Trust's ICT Infrastructure;
- withdraw or remove any material uploaded by that User in contravention of this Policy;
- disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith; or
- where the User is also a member of the Trust community, the Trust may take disciplinary action up to and including expulsion from study or termination of employment.

10. Monitoring

All Trust ICT systems and devices are monitored in accordance to policy, so personal privacy cannot be assumed when using trust hardware or systems. The Trust can monitor the usage of its own Infrastructure and services (internet access, email, teams, WiFi etc.) as well as activity on end user compute (Tablets, Laptops, Desktop computer, mobile phones etc.) without prior notification or authorisation from Users when justifiable concerns have been raised. This will be in line with the Trust's Investigation procedure

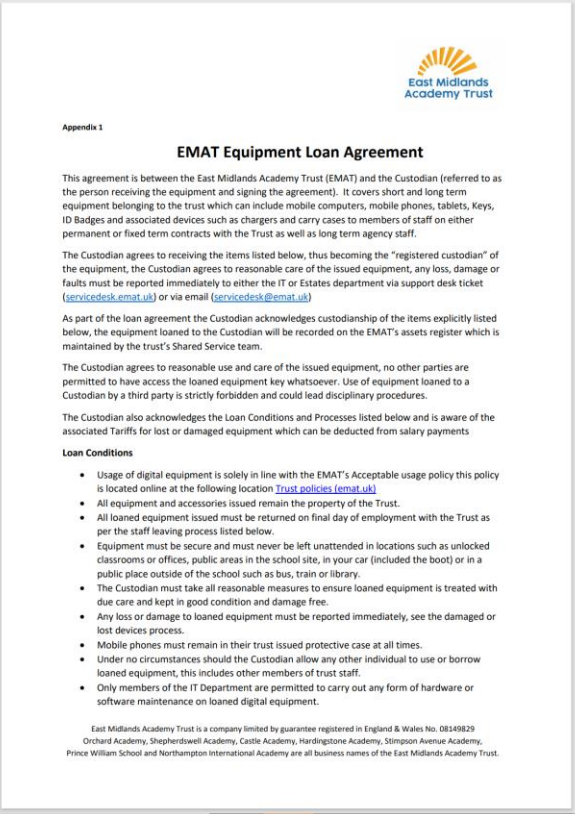
11. Definitions

ICT Infrastructure – all computing, telecommunication, software, services and networking facilities provided by the Trust either onsite at any of its Academies or related premises or remotely, with reference to all computing devices, either personal or Trust owned, connected to systems and services supplied by the Trust.

Users - any person granted authorisation to use any computer or device on the Trust ICT Infrastructure. This includes (but is not limited to) staff, students, visitors, customers (tenants or using site facilities), temporary workers, contractors, vendors, volunteers and sub-contractors authorised to access the network locally or remotely, for any reason, including email and Internet or intranet web browsing.

The Trust - refers to the East Midlands Academy Trust, Central Services and all Academies and sites associated with it.

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.



Appendix 1

EMAT Equipment Loan Agreement

This agreement is between the East Midlands Academy Trust (EMAT) and the Custodian (referred to as the person receiving the equipment and signing the agreement). It covers short and long term equipment belonging to the trust which can include mobile computers, mobile phones, tablets, Keys, ID Badges and associated devices such as chargers and carry cases to members of staff on either permanent or fixed term contracts with the Trust as well as long term agency staff.

The Custodian agrees to receiving the items listed below, thus becoming the "registered custodian" of the equipment, the Custodian agrees to reasonable care of the issued equipment, any loss, damage or faults must be reported immediately to either the IT or Estates department via support desk ticket (servicedesk.emat.uk) or via email (servicedesk@emat.uk)

As part of the loan agreement the Custodian acknowledges custodianship of the items explicitly listed below, the equipment loaned to the Custodian will be recorded on the EMAT's assets register which is maintained by the trust's Shared Service team.

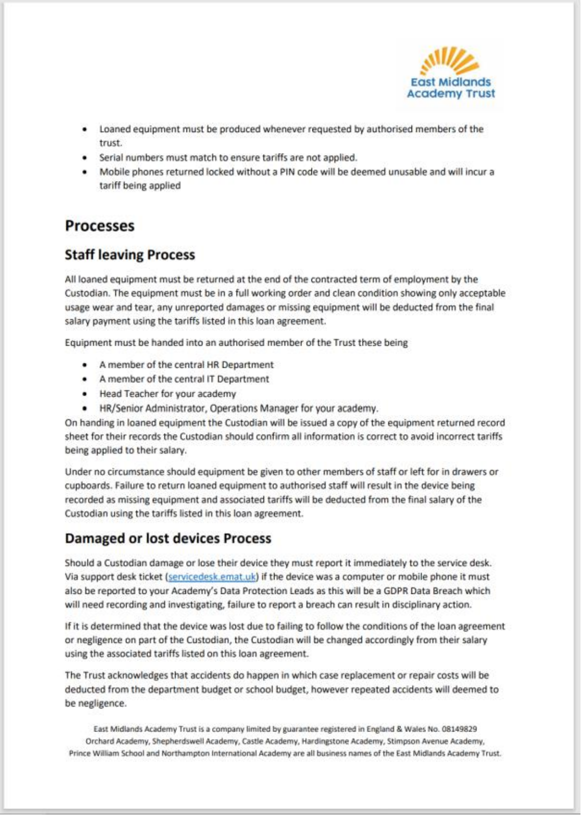
The Custodian agrees to reasonable use and care of the issued equipment, no other parties are permitted to have access the loaned equipment key whatsoever. Use of equipment loaned to a Custodian by a third party is strictly forbidden and could lead disciplinary procedures.

The Custodian also acknowledges the Loan Conditions and Processes listed below and is aware of the associated Tariffs for lost or damaged equipment which can be deducted from salary payments

Loan Conditions

- Usage of digital equipment is solely in line with the EMAT's Acceptable usage policy this policy is located online at the following location Trust policies (emat.uk)
- All equipment and accessories issued remain the property of the Trust.
- All loaned equipment issued must be returned on final day of employment with the Trust as per the staff leaving process listed below.
- Equipment must be secure and must never be left unattended in locations such as unlocked classrooms or offices, public areas in the school site, in your car (included the boot) or in a public place outside of the school such as bus, train or library.
- The Custodian must take all reasonable measures to ensure loaned equipment is treated with due care and kept in good condition and damage free.
- Any loss or damage to loaned equipment must be reported immediately, see the damaged or lost devices process.
- Mobile phones must remain in their trust issued protective case at all times.
- Under no circumstances should the Custodian allow any other individual to use or borrow loaned equipment, this includes other members of trust staff.
- Only members of the IT Department are permitted to carry out any form of hardware or software maintenance on loaned digital equipment.

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.



- Loaned equipment must be produced whenever requested by authorised members of the trust.
- Serial numbers must match to ensure tariffs are not applied.
- Mobile phones returned locked without a PIN code will be deemed unusable and will incur a tariff being applied

Processes

Staff leaving Process

All loaned equipment must be returned at the end of the contracted term of employment by the Custodian. The equipment must be in a full working order and clean condition showing only acceptable usage wear and tear, any unreported damages or missing equipment will be deducted from the final salary payment using the tariffs listed in this loan agreement.

Equipment must be handed into an authorised member of the Trust these being

- A member of the central HR Department
- A member of the central IT Department
- Head Teacher for your academy
- HR/Senior Administrator, Operations Manager for your academy.

On handing in loaned equipment the Custodian will be issued a copy of the equipment returned record sheet for their records the Custodian should confirm all information is correct to avoid incorrect tariffs being applied to their salary.

Under no circumstance should equipment be given to other members of staff or left for in drawers or cupboards. Failure to return loaned equipment to authorised staff will result in the device being recorded as missing equipment and associated tariffs will be deducted from the final salary of the Custodian using the tariffs listed in this loan agreement.

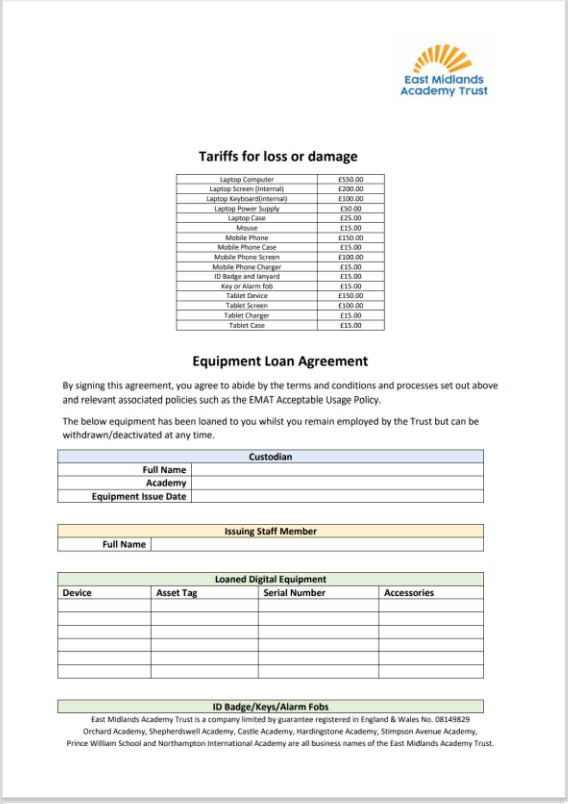
Damaged or lost devices Process

Should a Custodian damage or lose their device they must report it immediately to the service desk. Via support desk ticket (servicedesk.emat.uk) if the device was a computer or mobile phone it must also be reported to your Academy's Data Protection Leads as this will be a GDPR Data Breach which will need recording and investigating, failure to report a breach can result in disciplinary action.

If it is determined that the device was lost due to failing to follow the conditions of the loan agreement or negligence on part of the Custodian, the Custodian will be changed accordingly from their salary using the associated tariffs listed on this loan agreement.

The Trust acknowledges that accidents do happen in which case replacement or repair costs will be deducted from the department budget or school budget, however repeated accidents will deemed to be negligence.

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.



East Midlands Academy Trust

Tariffs for loss or damage

Laptop Computer	£550.00
Laptop Screen (Internal)	£200.00
Laptop Keyboard(internal)	£100.00
Laptop Power Supply	£50.00
Laptop Case	£25.00
Mouse	£15.00
Mobile Phone	£150.00
Mobile Phone Case	£15.00
Mobile Phone Screen	£100.00
Mobile Phone Charger	£15.00
ID Badge and lanyard	£15.00
Key or Alarm fob	£15.00
Tablet Device	£150.00
Tablet Screen	£100.00
Tablet Charger	£15.00
Tablet Case	£15.00

Equipment Loan Agreement

By signing this agreement, you agree to abide by the terms and conditions and processes set out above and relevant associated policies such as the EMAT Acceptable Usage Policy.

The below equipment has been loaned to you whilst you remain employed by the Trust but can be withdrawn/deactivated at any time.

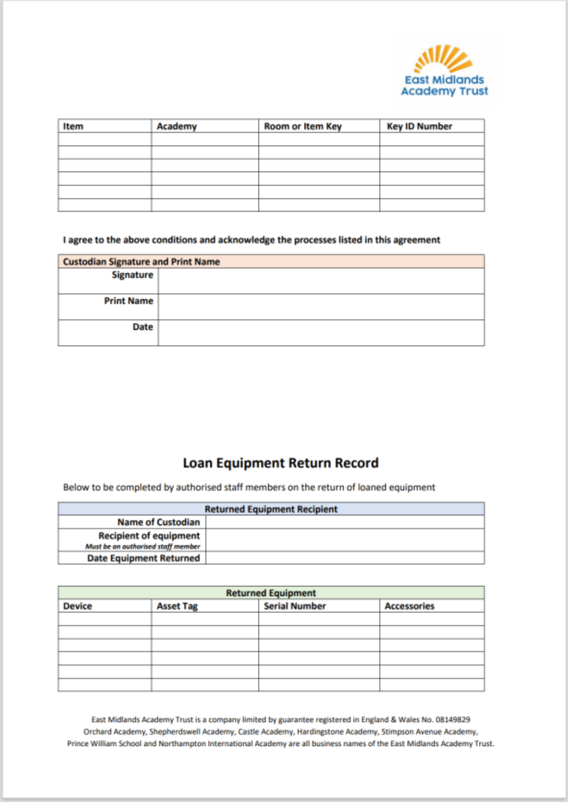
Custodian	
Full Name	
Academy	
Equipment Issue Date	

Issuing Staff Member	
Full Name	

Loaned Digital Equipment			
Device	Asset Tag	Serial Number	Accessories

ID Badge/Keys/Alarm Fobs

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.



East Midlands Academy Trust

Item	Academy	Room or Item Key	Key ID Number

I agree to the above conditions and acknowledge the processes listed in this agreement

Custodian Signature and Print Name	
Signature	
Print Name	
Date	

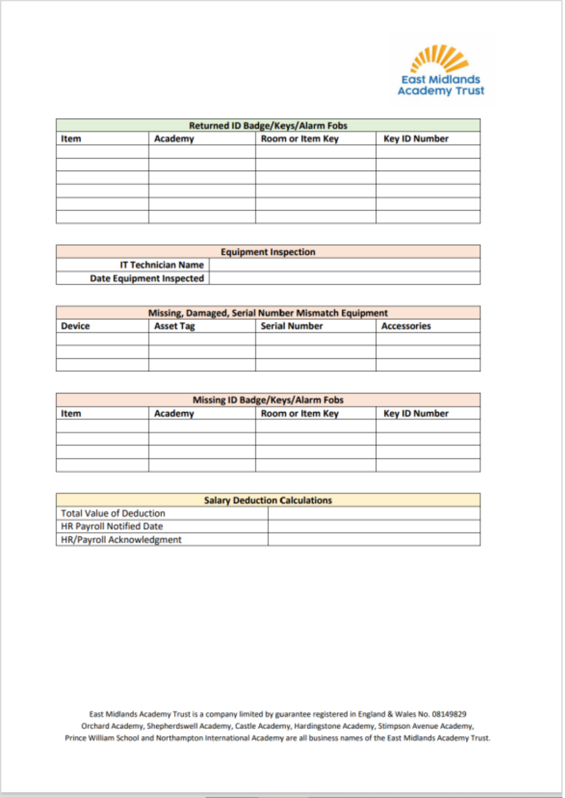
Loan Equipment Return Record

Below to be completed by authorised staff members on the return of loaned equipment

Returned Equipment Recipient	
Name of Custodian	
Recipient of equipment *Must be an authorised staff member*	
Date Equipment Returned	

Returned Equipment			
Device	Asset Tag	Serial Number	Accessories

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.



East Midlands Academy Trust

Returned ID Badge/Keys/Alarm Fobs			
Item	Academy	Room or Item Key	Key ID Number

Equipment Inspection	
IT Technician Name	
Date Equipment Inspected	

Missing, Damaged, Serial Number Mismatch Equipment			
Device	Asset Tag	Serial Number	Accessories

Missing ID Badge/Keys/Alarm Fobs			
Item	Academy	Room or Item Key	Key ID Number

Salary Deduction Calculations	
Total Value of Deduction	
HR Payroll Notified Date	
HR/Payroll Acknowledgment	

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.

	DfE Filtering and Monitoring Standards	

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems		
How to meet the standard	**Technical requirements**	**Evidence**
Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. To do this, they should identify and assign: - a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met - the roles and responsibilities of staff and third parties, for example, external service providers	The **senior leadership team** are responsible for: - procuring filtering and monitoring systems - documenting decisions on what is blocked or allowed and why - reviewing the effectiveness of your provision - overseeing reports - making sure that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns The **DSL** leads on safeguarding and online safety, including: - filtering and monitoring reports - safeguarding concerns - checks to filtering and monitoring systems The **IT service provider** has technical responsibility for: - maintaining filtering and monitoring systems - providing filtering and monitoring reports - completing actions following concerns or checks to systems	DSL's and senior leaders work closely together with EMAT IT service providers to meet the needs of each setting and to: - procure systems - identify risk - carry out reviews - carry out checks Roles and responsibilities are outlined in the EMAT Online Safety Policy and the EMAT Safeguarding and Child Protection Policy.

You should review your filtering and monitoring provision at least annually

How to meet the standard	Technical requirements	Evidence
Governing bodies and proprietors have overall strategic responsibility for making sure that filtering and monitoring provision is reviewed at least annually. The review should be conducted by members of the senior leadership team, the DSL, the IT service provider and involve the responsible governor. Results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.	Kay staff understand: - the risk profile of your pupils, including age range, pupils with SEND and pupils with EAL - what the filtering system currently blocks or allows and why - any outside safeguarding influences, such as county lines - any relevant safeguarding reports - the digital resilience of your pupils - teaching requirements (Eg, RHSE and PSHE curriculum) - the specific use of the chosen technologies, including Bring Your Own Device (BYOD) - what related safeguarding or technology policies are in place - what checks are currently taking place and how resulting actions are handled To make filtering and monitoring provision effective, the review informs: - related safeguarding or technology policies and procedures - roles and responsibilities - training of staff - curriculum and learning opportunities - procurement decisions - how often and what is checked - monitoring strategies The review is done as a minimum annually, or when:	Checks are undertaken jointly with DSL's, SLT and the EMAT IT service provider annually at the safeguarding forum. Staff are aware of the specific use of the chosen technologies such as BYOD as outlined in the EMAT IT Acceptable usage policy. The IT Acceptable usage policy is reviewed on an annual basis and is applicable to all ICT infrastructure users in the Trust. The EMAT IT service provider carries out checks at the start of each term. They confirm DNS (Domain Name System) settings and browser

	- a safeguarding risk is identified - there is a change in working practice, like remote access or BYOD - new technology is introduced The checks include a range of: - school owned devices and services, including those used off site - geographical areas across the site - user groups, for example, teachers, pupils and guests Records of checks include: - when the checks took place - who did the check - what they tested or checked - resulting actions Processes and systems ensure that: - all staff know how to report and record concerns - filtering and monitoring systems work on new devices and services before releasing them to staff and pupils - blocklists are reviewed and they can be modified in line with changes to safeguarding risks South West Grid for Learning's (SWGfL) testing tool is used to check that the filtering system is blocking access to: - illegal child sexual abuse material - unlawful terrorist content - adult content	extension deployment are correct. They run South West Grid for Learning (SWGfL tool in each deployment scenario / expected use. All information regarding the setup / demonstration / check results are stored in the 'EMAT All Staff' Teams folder for reference. All staff and stakeholders have received training to ensure they understand the filtering and monitoring systems and their roles and responsibilities in relation to filtering and monitoring. Specific training has been sent to DSLs and Deputy DSLs as part of Securly rollout and previously Senso rollout. Sample reports, Demo/training videos and a holistic overview of the filtering and monitoring setup is available in the 'EMAT All Staff' Teams folder.

Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning		
How to meet the standard	**Technical requirements**	**Evidence**
An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not: - unreasonably impact teaching and learning or school administration - restrict students from learning how to assess and manage risk themselves	The filtering provider is: - a member of Internet Watch Foundation (IWF) - signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) - blocking access to illegal content including child sexual abuse material (CSAM) / Child abuse image content (CAIC) The filtering system is operational, up to date and applied to all: - users, including guest accounts - school owned devices - devices using the school broadband connection The filtering system: - filters all internet feeds, including any backup connections - is age and ability appropriate for the users, and suitable for educational settings - handles multilingual web content, images, common misspellings and abbreviations - identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them - provides alerts when any web content has been blocked The providers filtering and monitoring system can be applied to devices using mobile or app content to reduce the risk of harm.	The filtering providers are Securly and Senso. Filtering for students is applied at a base level (fall-back) to all devices receiving a Dynamic Host Configuration Protocol (DHCP) assigned IP address, by way of issuing Securly DNS server addresses. Filtering is applied to Windows devices primarily by using a web browser extension for Microsoft Edge. Appropriate restrictions are deployed to client machines via Microsoft Intune Mobile Device Management (MDM) to prevent circumvention.

	The filtering systems allow key staff to identify: - device name or ID, IP address, and where possible, the individual - the time and date of attempted access - the search term or content being blocked EMAT conducts their own data protection impact assessment (DPIA) and reviews the privacy notices of third party providers. All staff are aware of reporting mechanisms for safeguarding and technical concerns. They report concerns if: - they witness or suspect unsuitable material has been accessed - they can access unsuitable material - they are teaching topics which could create unusual activity on the filtering logs - there is failure in the software or abuse of the system - there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks - they notice abbreviations or misspellings that allow access to restricted material	Securly is an educational provider. EMAT IT have built in the capability to differentiate settings between Primary and Secondary. Sites are blocked by categorisation. Image searches are appropriately restricted. The filtering service prevents access to websites serving VPN's and proxy services. Alerts are configured according to the filtering and monitoring overview document. Not all categories generate an alert (games for example). The categories that presently generate alerts are: Pornography, Drugs, Hate. Additional alerts are configured for Securly Aware, the wellness product. Securly: DOES NOT supply device name or IP address, as this is not possible for DNS

		filtering - all requests come from our external IPS. DOES supply the individual user account of the user where applicable. The time and date and search term or url category are supplied Senso: DOES supply device name DOES supply the individual user account of the user where applicable. (Not used as a filtering product - supplementary). The time and date and phrase logged are supplied. All staff have received training to ensure they are aware of reporting mechanisms for safeguarding and technical concerns.

		Roles and responsibilities along with guidance on reporting mechanisms for safeguarding and technical concerns are outlined in the EMAT Safeguarding and Child Protection Policy. Securely monitors a number of common foreign languages. Staff will support with physical supervision and will address cross language barriers through a risk assessment to mitigate risk.

You should have effective monitoring strategies that meet the safeguarding needs of your school or college		
How to meet the standard	**Technical requirements**	**Evidence**
Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.	The DSL takes lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. Training is provided to make sure both safeguarding and IT staff knowledge is current.	Key staff roles and responsibilities are included in the EMAT Safeguarding and Child Protection Policy and the EMAT Online Safety Policy.
Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include: - physical monitoring by staff watching screens of users - live supervision by staff on a console with device management software - network monitoring using log files of internet traffic and web access - individual device monitoring through software or third-party services	Device monitoring is managed by IT staff or third party providers, who: - make sure monitoring systems are working as expected - provide reporting on pupil device activity - make sure that monitoring data is received in a format that staff can understand - receive safeguarding training including online safety - record and report safeguarding concerns to the DSL - make sure that users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts	All staff have received training to ensure they are aware of filtering and monitoring systems, ensuring that incidents are urgently picked up, acted on and outcomes are recorded. Instructions and demo videos for generating Ad-Hoc reports for Securly have been provided to key staff.
	A technical monitoring system is applied to the devices mobile or app technologies that are used.	Monitoring procedures are reflected in EMAT Acceptable Use Policy and integrated, where applicable, into

	Technical monitoring systems do not stop unsafe activities on a device or online. Staff: - provide effective supervision - take steps to maintain awareness of how devices are being used by pupils - report any safeguarding concerns to the DSL	relevant EMAT Online Safety Policy, EMAT Safeguarding and Child Protection Policy and organisational policies, such as privacy notices. Securly and Senso both provide monitoring capability. Staff with appropriate access can use Senso to actively monitor screens of windows devices. This is usually only used by ICT teachers in secondaries. Data protection impact assessment (DPIA) and review of privacy notices of third party providers was carried out at Trust level as part of due diligence on procurement.

DfE Cyber Security Standards

Protect all devices on every network with a properly configured boundary or software firewall		
How to meet the standard	**Technical requirements**	**Evidence**
Properly configured firewalls prevent many attacks. They also make scanning for suitable hacking targets much harder. The IT service provider needs to set up your devices to meet the standards described in the technical requirements.	To meet this standard EMAT: - protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function - change the default administrator password, or disable remote access on each firewall - protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small specified IP-allow list combined with a managed password, or prevent access from the internet entirely - keep firewall firmware up to date - check monitoring logs as they can be useful in detecting suspicious activity - block inbound unauthenticated connections by default - document reasons why particular inbound traffic has been permitted through the firewall	- EMAT has network boundary security appliances. The manufacturer /model should be redacted from any public-facing documentation. Windows software firewall is on (default) on all devices. - Local administrator access on the security devices is restricted.

	- review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed - enable a software firewall for devices used on untrusted networks, like public wi-fi	- MFA is active on all accounts which have administrator access to the security appliance settings. - Firmware is updated as appropriate. - Monitoring logs are checked. - Inbound connections are blocked. - Inbound connections which are unblocked are limited to phone system support etc and specify the implied reason via the rule name. (Also limited to access via support provider's external IP). - There are no regular requirement to allow inbound connections. - Software firewalls on client devices are on for all networks

Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date		
How to meet the standard	**Technical requirements**	**Evidence**
Network devices include routers, switches, access points, servers and similar items. Recording network devices helps schools keep networks up-to-date and speeds up recovery.	To meet this standard EMAT: - keep a register, list, or diagram of all the network devices - avoid leaving network devices in unlocked or unattended locations - remove or disable unused user accounts, including guest and unused administrator accounts - change default device passwords - require authentication for users to access sensitive school data or network data - remove or disable all unnecessary software according to your organisational need - disable any auto-run features that allow file execution - set up filtering and monitoring services to work with the network's security features enabled - immediately change passwords which have been compromised or suspected of compromise - protect against a brute-force attack on all passwords by allowing no more than 10 guesses in 5 minutes, or locking devices after no more than 10 unsuccessful attempts	- EMAT have appropriate documentation for network topology. Network hardware is confined to restricted access rooms / cabinets etc where possible. Additionally, no "core" hardware changes are configured without prior approval of IT Business Partner or Head of Shared Service with good justification. - Account disablement is automatic when students are leavers on SIMS/Arbor. Similarly Account set up for new admissions on SIMS/Arbor. - All data storage in sharepoint requires user authentification. External systems e.g Arbor require user authentication.

	If network devices have conflicting security features, decisions on which security features have been enabled or disabled on the network are documented. To physically access switches and boot-up settings a password or PIN of at least 6 characters is used. The password or PIN is only be used to access this device. For all other devices, password strength at the system level is enforced. If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test. Password manager software is recommended.	- Unneeded applications are removed to reduce client device attack surface. - Auto-run is disabled - Suspected compromised accounts are actioned immediately. - Password lockout is not required as devices are not connected to a local domain. - Filtering on network boundary security devices has been disabled (except for specific security-related setup). This allows traffic to hit Securly servers. Without this configuration, access to filtered websites would be blocked before reaching the main filtering and monitoring solution, which would prevent alerts and reports being available to safeguarding teams. - Cloud managed password strength system is in place. The Trust is reviewing a suitable Password Manager software solution

		and will determine within the academic year 2023/2024 if this recommendation is to be implemented
Accounts should only have the access they require to perform their role and should be authenticated to access data and services		
How to meet the standard	**Technical requirements**	**Evidence**
Successful cyber attacks target user accounts with the widest access and highest privileges on a network. You must limit the numbers and access of network and global administrative accounts. There must be a user account creation, approval and removal process. You should make this part of school joining and leaving protocols.	Only authorised people have an account which allows them to access, alter, disclose or delete the held personal data. Users have a separate account for routine business, including internet access, if their main account: - is an administrative account - enables the execution of software that makes significant system or security changes - can make changes to the operating system - can create new accounts - can change the privileges of existing accounts Password strength is enforced at system level.	- Account permissions were reviewed during Arbor transfer process (Summer 2023) - Account disablement is automatic when students are leavers on SIMS/Arbor. Similarly Account set up for new admissions on SIMS/Arbor. - 365 has automatic blocking of common passwords as default

	If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test. The National Cyber Security Centre recommends using passwords made up of 3 random words. Enforce account lockouts after a number of failed attempts and require service provider or network manager permission to unlock. Any password that has been compromised or suspected of compromise is immediately changed. Accounts of users who have left their employment, or accounts that have not been used for a prolonged period of time are reviewed termly and removed. Unused role privileges are removed or disabled. No user’s account has more access to devices than required to carry out their role. Different accounts have specific rights for different purposes. IT service providers and administrators enable just-in-time access, giving individual users time-limited privileges as required.	

You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication

How to meet the standard	Technical requirements	Evidence
Multi-factor authentication only allows access to a service when you present 2 or more different forms of authentication.	All staff are strongly encouraged to use multi-factor authentication. Multi-factor authentication includes at least 2 of the following: - passwords constructed in the formats described earlier in standard 3 - a managed device, that may belong to the organisation - an application on a trusted device - a device with a trusted network IP address, you should not use this in MFA for accounts with administrator rights or for accessing sensitive data - a physically separate token - a known/trusted account, where a second party authenticates another's credentials - a biometric test	- All EMAT central team staff have MFA configured. - There is an open project to rollout MFA to all teaching staff (and select other staff) via hardware token. - Training is provided to users unfamiliar with multi-factor authentication.

You should use anti-malware software to protect all devices on the network, including cloud-based networks

How to meet the standard	Technical requirements	Evidence
Up-to-date anti-malware and anti-virus software reduces the risk from many forms of cyber attack. Some applications protect against viruses and general malware, some against one only. You need to protect against both.	Anti-malware software and associated files and databases are kept up to date. Anti-malware software: - is set up to scan files upon access, when downloaded, opened, or accessed from a network folder - scans web pages as they are accessed - prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement	Sophos is deployed to all client devices

An administrator should check the security of all applications downloaded onto a network

How to meet the standard	Technical requirements	Evidence
Applications can insert malware onto a network or have unintentional security weaknesses. Users should not download applications. The IT service provider should check them first.	The EMAT IT service provider approves all code and applications that are deployed and makes sure they do not pose a security risk. A current list of approved applications is maintained. Applications with invalid or no digital signatures are not be installed or used. The network's anti-malware service is scanning all downloaded applications.	All software is deployed via Intune Mobile Device Management (MDM). Intune>Apps forms the approved applications list at present. Sophos scans all downloads. There is an open project to rollout Windows Defender Application Control to client devices.

All online devices and software must be licensed for use and should be patched with the latest security updates		
How to meet the standard	**Technical requirements**	**Evidence**
You must not use unlicensed hardware or software. You must avoid or replace unpatched or unsupported hardware or software, including operating systems. Subscribing to services rather than buying items can be a way to help achieve this. This is known as Software as a Service (SaaS). So that appropriate risk assessment and mitigation can take place, your IT service provider should tell leadership and governors at the school or college and alter the network accordingly when devices or software: - have become unsupported - are about to become unsupported	All software is currently licensed. Unsupported software is removed. Unsupported devices only access segmented areas of the network which do not grant access to sensitive data. Automatic updates are enabled. Manual updates to hardware or software are completed, including configuration changes, within 14 days of the release of the patch where the vulnerability is: - described as high risk or worse - has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above When notified by the Department for Education (DfE), patches are applied within 3 days of notification.	Intune supports all actions. This is monitored by EMAT IT.

You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site		
How to meet the standard	**Technical requirements**	**Evidence**
A backup is an additional copy of data, held in a different location, in case the original data is lost or damaged. If all copies were held in the same location, they would all be at risk from natural disasters and criminal damage. The safest way to achieve this is to have a pattern of backing up on a rolling schedule. You should keep these backups off the network when not in use and check them regularly.	There are at least 3 backup copies of important data, on at least 2 separate devices. At least 1 of these copies is kept off-site. Backups are scheduled regularly. At least 1 of the backups must be offline at all times (cold backup). Where the cloud services allow it, set up controls: - only allow authorised devices to create new or appended backups - deny connection requests when backup is not in use Processes are in place to regularly check that the backups work.	Local backups are less relevant as all data has moved to cloud storage. Cloud storage is backed up via a 3rd party supplier on a regular schedule. Due to the presence of Versioning and 2-stage recycle bins, restoration activity is rarely requested. It can be completed within a short timeframe if required, dependant on the size of the data requested. Barracuda cloud supports backup processes. The Trust currently uses an alternative solution to off line backups called immutable backups. The back up strategy is being reviewed in 2023/2024 and an offline

		backup solution will be in place before the end of the academic year.
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack		
How to meet the standard	**Technical requirements**	**Evidence**
Effective response will reduce the material, reputational and safeguarding damage from ransomware attacks. Make sure you have a cyber attack contingency plan. The plan must be part of your business continuity and disaster recovery plan. The school's governors should ensure the creation and testing of these plans. In multi-academy trusts, oversight might happen at trust level.	School contingency plan are in place and include: - staff responsibilities - out of hours contacts and procedures - internal and external reporting and communications plans - priorities for service restoration - the minimum operational IT requirements - where you can find additional help and resources Hard copies of key information are kept in case of total system failure. Plans are regularly tested and reviewed.	Business Contingency Plan is in place and identifies key roles and responsibilities.

Serious cyber attacks should be reported		
How to meet the standard	**Technical requirements**	**Evidence**
A cyber attack is defined as an intentional and unauthorised attempt to access or compromise the data, hardware or software on a computer network or system. An attack could be made by a person outside or inside the school. This compromise of data might include: - stealing the data - copying the data - tampering with the data - damaging or disrupting the data, or similar unauthorised access Where a data breach has or may have occurred, report to the Information Commissioner’s Office (ICO). These incidents should also be reported to the DfE sector cyber team at Sector.Incidentreporting@education.gov.uk. Academy trusts have to report these attacks to ESFA.	When reporting cyber attacks, EMAT acts in accordance with: - Action Fraud guidance for reporting fraud and cyber crime - ESFA Academy Trust Handbook Part 6 - ICO requirements for reporting personal data breaches	EMAT will follow referenced guidance if required.

You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation		
How to meet the standard	**Technical requirements**	**Evidence**
The protection of sensitive and personal data is vital to: - the safety of staff and students - the reputation of schools and colleges - the confidence placed in schools and colleges - avoid the legal liabilities which security breaches expose schools and colleges to	EMAT ensures that it: - understands the definition of personal data - assesses the risk of compromise, and the degree of damage caused by a security compromise, to work out the resources required to protect the data - any personal data is pseudonymised or encrypted while stored and in transit to a third party - ensures the confidentiality, integrity and availability of the data and systems processing them - restores complete and accurate data after an incident in a timely fashion - designs and applys processes for testing and assessing the effectiveness of all measures used to safeguard data and its use The risk assessment is incorporated into the risk register. Encryption to protect data: - uses strong encryption - uses encryption systems that are still supported - has a life appropriate to the sensitivity of the data being stored	All staff complete GDPR training. In line with GDPR (UK) law this compliance is monitored by the Head of Shared Service and reported to Trustees and LAB members as well as reported in the trusts Financial Scrutiny meetings. The Data Protection Lead (DPL) in each academy is responsible for ensuring staff follow best practice such as minimisation and pseudonymisation of data and the appropriate methods for sharing data. Data protection and compliance to GDPR is explicitly recorded in the Trusts Risk Register and is an agenda item in every Audit and Risk Committee Trustee meeting held three times a year.

		All EMAT devices are encrypted with supported technologies. Data retention policy exists and is followed for the retention of personal data.

Train all staff with access to school IT networks in the basics of cyber security

How to meet the standard	Technical requirements	Evidence
Basic cyber security knowledge amongst staff and governors is vital in promoting a more risk aware school culture.	Staff and governors receive annual basic cyber security training which focuses on: - phishing - password security - social engineering - the dangers of removable storage media The training is part of the induction training for new staff.	All staff with access to the IT network are mandated to undertake NCSC Cyber Security Training for Schools annually. At least one member of the governing body has completed the training. Governors completing the training have read the NCSC publication school cyber security questions for governors.