GMET
Greater Manchester
Education Trust

Greater Manchester Education Trust

ONLINE SAFETY, TECHNICAL SECURITY AND SOCIAL MEDIA POLICY

V2.0

Approval History

Approved By:	Date of Approval	Version Approved	Comments
Finance, Audit and Resources Committee	3.7.2023	V1.0	New Version
Finance, Audit and Resources Committee	April 2025	V2.0	Revised Version

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Owner/Editor
April 2025	July 2023	Updated with changes to personnel and any relevant changes in technology settings e.g. use of central management software system for managing iPads and other portable devices.	C Wragg

CONTENTS

APPENDICES

1. Rationale

Within the Greater Manchester Education Trust (GMET), we believe that the use of technology is an essential part of education in the 21st century. We are immersed in a digital world where systems are available 24 hours a day and where the proliferation of personal devices means that people use a variety of platforms and media to communicate, organise and teach.

Whilst the use of technology offers benefits, there are risks and unfortunately some adults and young people may expose themselves to danger either knowingly or unknowingly. In the light of the rapid evolution of IT systems and social networking technologies, the Trust requires a robust policy framework so that all adults working in the academies are aware of the Trust's expectations and the rules they are expected to follow when using IT equipment and systems and social media platforms both inside and outside of the academy environment in order to protect themselves, the students in their care and the reputation of the academy and the wider Trust.

2. Statement of intent

This policy defines the expectations for the provision and use of IT for staff at the Greater Manchester Education Trust (GMET). Its purpose is to: ensure that the Trust meets the requirements on schools with regard to technical security and safeguarding, support the use of IT for effective working and communication; encourage the creative use of technology to engage learners; minimise the risks to students and staff of inappropriate situations and materials; protect the staff, the academy and the Trust from litigation and to minimise the risks to the IT network and systems. It is designed to guide adults in their use of IT equipment, services and social media platforms responsibly in order to safeguard the Trust, the individual academies, students, staff, academy governors, Trustees and members of the wider academy communities.

This policy should be read in conjunction with other relevant Trust and academy policies in particular, the Trust's Safeguarding Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy

The principles which underpin this policy are:

- The Trust is committed to utilising technology to support learning and working practices.
- The Trust will provide a robust and secure environment which adheres to the guidance described in:
  - Keeping Children Safe in Education (DfE)
  - Meeting digital and technology standards in schools and colleges (DfE)
  - Appropriate filtering and monitoring (UKSIC)
- Adults are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions.

- Adults must continually monitor and review their own practices in terms of the continually evolving world of technology, systems and social networking and ensure that they consistently follow the rules, principles contained and guidance mentioned in this policy.
- The use of IT within the Greater Manchester Education Trust is underpinned by the term ‘Unacceptable Use’.

3. Legal framework and guidance

This policy takes into account the latest provisions of:

Department for Education

- Keeping Children Safe in Education (Statutory)
- Meeting digital and technology standards in schools and colleges (Advisory)
- Cyber Security standards for schools and colleges (Advisory)

The Home Office

- The Prevent Duty: safeguarding learners vulnerable to radicalisation

UK Safer Internet Centre

- Appropriate filtering and monitoring: A guide for education setings and filtering providers
- Test Your Internet filter
- Online safety in schools and colleges: Questions from the Governing Board (2022) – (as signposted by the DfE)

4. Scope and definitions

This policy applies to all adults working for the academy or Trust community (including staff, contractors, volunteers, and community users) who have access to and are users of academy digital systems, both in and out of the academy. It also applies to the use of personal digital technology on the academy site (where allowed). This policy also applies to Trust and academy governors and Trustees. There are descriptions in this policy relating to student behaviour, these are to illustrate to adults how the use of technology applies to students in order for adults to contribute to a safe and robust learning environment.

This policy deals with the use of IT facilities and associated web-based services across the Trust, external systems (including social media platforms), academy owned devices, personal devices used for academy or Trust related use and applies to all academy employees, and authorised adult users. It covers the personal use of social media as well as the use of social media for professional use and/or academy purposes (whether official or not), including the use of websites and services hosted and maintained on behalf of the academy.

This policy covers the use of IT equipment and social media as defined in this policy and also personal blogs and any posts made on other people's blogs and to all on line forums and notice boards. The guidance, rules and principles set out in this policy must be followed irrespective of the device, platform or medium.

In this policy, the following definitions apply:

a. **unacceptable use** - is defined as any activity which is; conducted without permission, outside the specific learning aim for that lesson or activity, illegal, considered extreme or radicalising, dangerous, vexatious or where the equipment is used to make any student, member of staff or member of the public feel uncomfortable or vulnerable.
b. **IT equipment and services** – means any device, network, software system or other digital resource used for academy or Trust related business irrespective of the ownership of that device.
c. **personal use** - means any activity, account or system used privately for home, leisure or other interests which do not relate to the academy, the Trust or business other than education.
d. **professional use** - means any activity, account or system that is used for any business related to education, employment area or where you are maintaining a presence in a professional capacity.
e. **Trust use** – means any account set up on behalf of the Trust, an academy, a department or an individual which is designed to reflect the opinions and values of the academy or the Trust.
f. **social media/social networking platforms** - means any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Social media includes but is not limited to, online social forums such as Twitter, Facebook and LinkedIn; messaging services such as WhatsApp and Messenger; and also covers blogs, chat rooms, forums, podcasts and video- image-sharing websites such as YouTube, TikTok, Snapchat, Instagram, Reddit, Pinterest and Tumblr. (The internet is a fast-moving technology and it is impossible to cover all examples of emerging social media in this policy.)
g. **adults/adults working in academy** - means all members of staff (including teaching and non-teaching staff) who work for the Greater Manchester Education Trust as an employee or on a self- employed basis. It also includes trainee teachers, other trainees and apprentices, volunteers, agency staff, external consultants, trustees and academy governors.
h. **information** - means all types of information including but not limited to, facts, data, comments, audio, video, photographs, images and any other form of online interaction.
i. **inappropriate information** - means information (as defined above) which any reasonable person would consider to be unsuitable or inappropriate in the

circumstances and considering the adult's position within the academy.

j. **the Trust, the academy and the wider academy community** - means the Greater Manchester Education Trust, any academy designated as part of the Trust, any student, parents/carers of students, former students of any academy in the Trust, any adult that is, or has been, employed by the Greater Manchester Education Trust and any other person or body directly or indirectly connected with the Trust or any of its member academies.
k. **A**I – means Artificial Intelligence and refers to is the development of systems that are able to perform tasks normally requiring human intelligence. Generative AI means any system which is used to generate new content in response to input, based on large data models that the system has been trained on. E.g. ChatGPT

5. Roles and responsibilities

The Trust Board is responsible for ensuring that its employees, governors and Trust directors act in a lawful manner, making appropriate use of academy technologies for approved purposes only.

The Trust Board or delegated group is responsible for overseeing relevant policies and the Academy Headteacher is responsible for ensuring that staff at their academy are aware of their contents.

The Academy Headteacher has a duty of care for ensuring the safety (including online safety) of members of their academy community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety, which may be delegated to authorised staff.

The Academy Headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal online safety monitoring role. The Academy Headteacher is also responsible for ensuring an inventory of IT equipment is recorded as part of the academy asset management register.

If the Headteacher or Chief Executive Officer has reason to believe that any IT equipment and services have been misused by an adult, they will consult the Trust's Director of People for advice without delay. The Director of People will agree with the Headteacher or Chief Executive Officer on an appropriate strategy for the investigation of the allegations and liaise with other agencies as appropriate. Incidents will be investigated in a timely manner in accordance with agreed procedures. The Headteacher and Chief Executive Officer will make it clear that internal academy staff should not carry out any investigations unless they are both qualified and authorised to do so.

The Headteacher and the Trust will:

a. provide IT equipment and services with appropriate functionality and security mechanisms and ensure that all adults working in academy are familiar with this policy and any related policies.
b. take all reasonable steps to enable adults to work safely and responsibly and to

support safer working practice in general with regard to the use of the IT equipment and services, the internet and other communication technologies.

c. publish guidance around the use of IT and online safety to support staff in their day-to-day work
d. ensure appropriate filters and monitoring systems are in place.
e. set clear rules in relation to the expected standards of behaviour whilst using relevant IT equipment and services and social networking platforms for personal, professional or Trust use.
f. give a clear message that unlawful or unsafe behaviour or practice is unacceptable and that where appropriate, disciplinary, legal and/or other action will be taken.
g. provide support to staff experiencing digital issues in relation to their workplace (where possible)
h. ensure that all concerns raised in relation to the misuse of Trust or academy IT equipment and services, and social media sites are investigated promptly and appropriately.
i. ensure procedures are in place to handle allegations against any adult.
j. take all reasonable steps to minimise the risk of misplaced or malicious allegations being made against adults working in academy.
k. take all reasonable steps to prevent adults working in academy abusing or misusing their position of trust.

The Designated Safeguarding lead will:

a. liaise with the Digital Strategy Lead to ensure that appropriate roles and responsibilities are in place to manage filtering and monitoring systems
b. annually review filtering and monitoring systems for their academy

Adults working in academy must:

a. understand that digital and online safety are core parts of safeguarding
c. ensure they are familiar with the contents of this policy and the accompanying guidance.
d. adhere to and apply the rules and principles in this policy in all aspects of their work and in their personal time.
e. act in accordance with their duties and responsibilities under this policy and the statutory/ non statutory advice and guidance referred to.
f. demonstrate high standards of personal and professional conduct when using IT equipment and services (including generative AI platforms), and social media platforms.
g. only use the IT equipment and services for which they have authorisation.
h. use IT equipment and services only for their intended purpose.
i. use appropriate channels of communication and pay regard to the information being communicated.
j. take reasonable steps to protect the access and integrity of all IT equipment and services.
k. respect the privacy and personal rights of others.
l. never, in any circumstances, abuse or misuse their position of trust.

m. raise any concerns or queries in connection with this policy with the academy Headteacher.
n. be alert for signs of unacceptable use of IT, cyber-bullying, exploitation or radicalisation and report concerns immediately through the appropriate academy systems.
o. engage with any training provided or facilitated by or the academy in relation to the use of the internet or any other online, digital or communication technologies.

Key personnel	Digital Lead	Designated Safeguarding Lead
LHS	Mrs Catherine Wragg	Ms Donna Johnson
PWHS	Mrs Catherine Wragg	Mrs Michelle Dean
TEMA	Mrs Catherine Wragg	Ms Gill Houghton
WRHS	Mrs Catherine Wragg	Ms Morresa Connolly

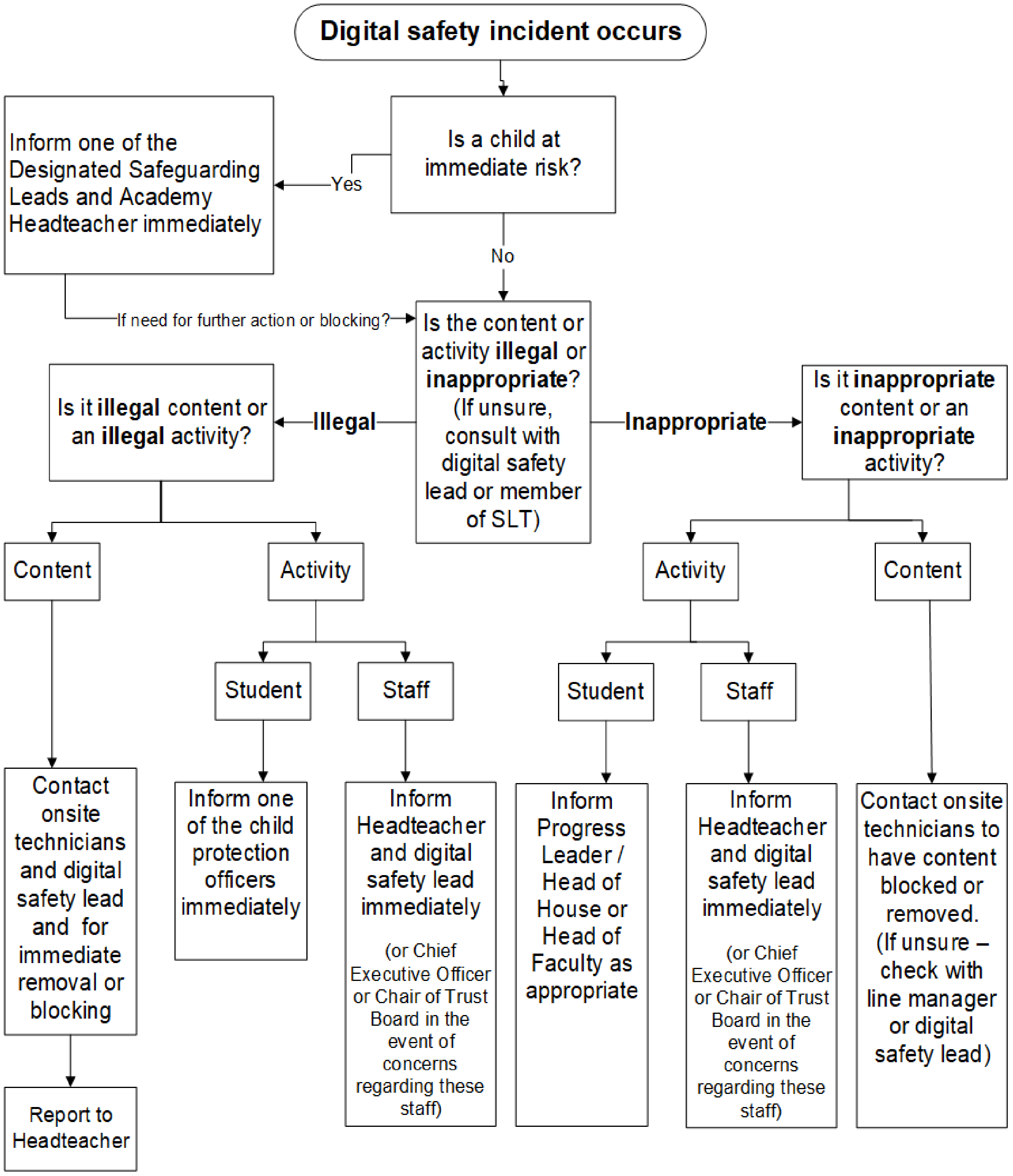
The policy must be read in conjunction with the Data Protection Policy, the Safeguarding Policy, the Digital Guidance document and the Staff Code of Conduct

6. Reporting

Staff are responsible for reporting every breach of the Online Safety policy. If a member of staff knows, or suspects, that a colleague is in breach of any part of this policy he/she must report it to the appropriate person in writing by email to the following leads and copy in the academy Headteacher.

It is also important to recognise that digital safety is not an IT issue. It may involve the use of IT, but it is about protecting children, young people and adults from harm. This policy relates to staff but the reporting mechanisms outlined below also relate to students for clarity and ease of use. If a member of staff has concerns about the behaviour of a young person in relation to IT systems or services, they should follow the mechanisms outlined in the Safeguarding and/or Behaviour policies. If you have a concern about actual, significant harm to a child or young person, or the risk of significant harm, then you should make immediate contact with the Child Protection / Safeguarding Officers in the academy.

Timescale:	Incident:	Report to:	Method
Immediate reporting:	Illegal activity by student or illegal content viewed or shared by student	Child Protection / Safeguarding Team	CPOMS
	Illegal or inappropriate activity by a member of staff	Headteacher and Digital Lead	Email
	Illegal or inappropriate activity by the Headteacher or Cross-Trust staff	Chief Executive Officer	Email
	Illegal or inappropriate activity by Chief Executive Officer	Chair of Trust Board	Email
	Illegal content or material which requires **immediate** removal or blocking	Onsite technicians and Child Protection / Safeguarding Team	Email
Same day reporting:	Inappropriate material which requires additional filtering on the internet	Onsite technicians and Digital Lead	Email
	Inappropriate activity by a student in a lesson (which does not constitute a Child Protection / Safeguarding incident)	Heads of Faculty/Subject or Pastoral Leads as appropriate to the behaviour policy	SIMS (or designated behaviour system)
	Inappropriate activity by a student not in a lesson (which does not constitute a Child Protection / Safeguarding incident)	Heads of Year / Progress Leaders / Pastoral Leads as appropriate to the behaviour policy	SIMS (or designated behaviour system)


Digital safety incident occurs
Is a child at immediate risk?
Yes
Inform one of the Designated Safeguarding Leads and Academy Headteacher immediately
No
If need for further action or blocking?
Is the content or activity **illegal** or **inappropriate**? (If unsure, consult with digital safety lead or member of SLT)
Illegal
Inappropriate
Is it **illegal** content or an **illegal** activity?
Is it **inappropriate** content or an **inappropriate** activity?
Content
Activity
Activity
Content
Student
Staff
Student
Staff
Contact onsite technicians and digital safety lead and for immediate removal or blocking
Report to Headteacher
Inform one of the child protection officers immediately
Inform Headteacher and digital safety lead immediately (or Chief Executive Officer or Chair of Trust Board in the event of concerns regarding these staff)
Inform Progress Leader / Head of House or Head of Faculty as appropriate
Inform Headteacher and digital safety lead immediately (or Chief Executive Officer or Chair of Trust Board in the event of concerns regarding these staff)
Contact onsite technicians to have content blocked or removed. (If unsure – check with line manager or digital safety lead)

Any incident involving a concern about a student must be formally recorded on CPOMS and/or SIMS. The headteacher or appropriate senior staff will make the decision about contact with parents.

Any incident concerning a member of staff must be reported by email to the appropriate person

7. Breaches of policy and other issues

a. Any breach of this policy and the duties, responsibilities, professional standards and legal obligations referred to will be regarded as a serious matter and action including disciplinary action in appropriate circumstances will be taken by the Headteacher (or the Academy Committee or Trust Board). In serious cases involving employees this may lead to dismissal without notice on the grounds of gross misconduct.

b. Where there has been a breach of this policy, the academy will also take whatever action is considered appropriate in order to protect the reputation and integrity of the academy, the Trust and the wider academy community.

c. Adults must be aware that any breach of this policy involving a breach of the laws, professional codes or other statutory provisions referred to in this policy may result in legal or other action being taken against them by a body or person other than the academy.

8. Further information and guidance

a. Guidance relating to the use of IT equipment and services, and social media is published in a separate document.
b. Electronic guides and training are available via the links on the academy Intranet
c. Further clarification can be requested by contacting the Trust Digital Strategy Lead cwragg@gmetrust.org

Appendix A: Technical Security, Systems and monitoring

Technical Security:

Each academy will be responsible for ensuring that the onsite infrastructure/network is as safe and secure as is reasonably possible, as directed by the Trust Director for IT Infrastructure and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- Academy technical systems will be centrally overseen, but locally managed in ways that ensure that the academy is able to adapt to local need, whilst meeting recommended technical requirements

- There will be regular reviews and audits of the safety and security of Trust and academy technical systems conducted centrally by Trust staff in conjunction with onsite staff and periodically validated by external auditors

- Servers, wireless systems, and network switching must be securely located and physical access to these locations must be restricted

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

- The academy's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from malware, viruses, worms, trojans etc.

- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff

- All users will have clearly defined access rights to academy technical systems these security settings (for each person) are based upon role and/or group membership and these technical settings are agreed by the Trust IT Director and Infrastructure Team in conjunction with the academy Headteacher/Digital Strategy Lead and are managed operationally by the onsite IT technicians

- Bespoke permissions are agreed with the Chief Executive Officer, Academy Headteacher or Digital Strategy Lead as necessary

- Temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the academy's systems is permitted and can be arranged through reception or the onsite technicians. Temporary logins are limited to 24hrs by default but can be extended up to 1 week if needed. Beyond one week, the visitor should be set up with an individual, named account.

- The Trust Director of IT Infrastructure is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the academy to breach the Copyright Act which could result in fines or unexpected licensing costs)

- Staff are not permitted to download or install executable files or install programmes on computers or laptops. Exceptions may be made for certain signed applications within approved ‘app stores’ on mobile devices.

- Staff are permitted to install licensed apps on their staff iPad or other mobile handset for Trust or personal use provided the app is appropriate to the use of a work device and that which any reasonable person would consider to be suitable or appropriate in the circumstances and considering the adult’s position within the academy. For example, it would be considered suitable to install a streaming app such as BBC iPlayer but not an app to access pornography

- Academy owned devices will be enrolled onto Trust managed Mobile Device Management platforms (MDMs) such as Intune or JAMF School, by the IT technicians to receive policies, security and Wi-Fi settings to allow them to connect automatically when brought onto academy premises but those deemed allowed for outside use will further be permitted to connect to other Wi-Fi networks by the user when taken off site

- Staff and students are permitted to use their own personal IT equipment on any academy grounds, at the discretion of the Headteacher or Chief Executive Officer – Subject to appropriate internet and firewall filtering policies.

- If personal devices are allowed for students, they are only allowed to use them in lessons/learning activities at the discretion of the adult supervising the activity

- A helpdesk system is in place for staff to report any actual/potential technical incident to the onsite technicians and this is overseen by the Trust Director of IT Infrastructure and Trust Engineer

- Where possible, the Trust will endeavour to implement single sign on authentication (SSO) with Microsoft or Google platforms where this option is technically achievable within a system.

- Where users request the ability to sign in with their Trust Microsoft account, this will be permitted for known software (already on the list). Where this is not the case, all requests to create a single sign on will automatically be paused whilst due diligence is carried out. The Trust reserves the right to refuse permission for the creation of single sign on where they are concerned about the data protection implications of the account creation.

- Where possible, the Trust will deploy multi-factor authentication on remote services where personal data may be stored such as email, the remote desktop and Microsoft 365

Passwords:

- These statements apply to all users.

- All academy-owned devices, academy networks and systems will be protected by secure passwords.

- Logins/accounts for the academy network and services are automatically created when a new member of staff or student is recorded in SIMS. In some circumstances, other users can have individual accounts created, but this must be agreed with the Headteacher.

- Accounts are disabled immediately when a user leaves the employment of the Trust – accounts are then in turn deleted at the end of that half term. Staff accounts occasionally remain accessible to designated persons if required. Where a staff account is retained for an extended period e.g. a leaving CP officer, the account will be 'frozen' with access restricted to personnel as directed by the headteacher.

- Users will be made responsible for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see password section below)

Password requirements:

- Passwords should be long. Good practice will be given to all staff on enrolment and all staff will periodically be reminded of good password hygiene. Technical policies are also enforced to ensure complexity is adhered to and known 'exposed' passwords are also blocked from use.

- Passwords cannot include names or any other personal information about the user that might be known by others and will be referenced against a password deny lists recommended by the National Cyber Security Centre and exposed list by HaveIBeenPwned. Passwords that are deemed vulnerable will be denied unless there is a specific need for a vulnerable student in which case the technicians will advise on a suitable password in conjunction with SEND staff

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the academy

- Passwords must be changed on first login to the system

- Staff passwords expire after 1 year and student passwords expire after 2 years unless a password breach has occurred, in which case, a user or group of users will be required to change their password at next logon.

- Records of learner usernames and passwords for SEND or vulnerable learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.

Notes for technical staff/teams:

- Each administrator will have an individual administrator account, as well as their own day to day user account with access levels set at an appropriate level. Two factor authentication for all such accounts will be strictly employed. Administrator lockout policies are also much stricter. In the event of any locked admin account, it takes another admin to investigate and remove the lock.

- All digitally stored admin-level credentials are secured within a restricted-access area and further protected using Microsoft 365 Information Rights Management (IRM) with AES-256 encryption. This ensures strong security, controlled access and auditability, preventing unauthorised sharing, printing or compromise.

- Suitable arrangements are in place to provide visitors with appropriate access to systems which expires after use.

- A standard user account is "locked out" following five successive incorrect log-on attempts on desktop computers. This is subsequently unlocked after a period of 5 minutes, however repeated locking results in alerts being sent to the IT team for additional investigation. On mobile devices such as iPads, when an incorrect PIN or password is repeatedly entered the device enforces an increasing lockout period to prevent unauthorised access. After several failed attempts the wait time gradually increases from 1 minute to 1 hour, whereas on the 10th failed attempt the device will fully erase and remain locked until returned to an IT team member.

- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).

Internet Filtering:

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this academy.

- All internet traffic for academy owned devices will be directed through the academy/Trust cloud-based web filter whether the device is onsite or offsite

- Internet traffic will be filtered by a company which is recognized by the UK Safer Internet Centre and which demonstrates that our systems filter appropriately using http://testfiltering.com/ as recommended by the DfE

- Staff and students will receive different Internet profile policies to allow for more bespoke management and student profiles can be further divided if needed under the direction of the Trust Digital Strategy Lead, the DSL, members of SLT and the Headteacher

- Filtering standards will be established as described by the UK Safer Internet Centre

- All websites categorised as copyright breach, phishing, VPN, pornography, gambling, security risks and violence will be centrally blocked for all as a default. Any member of staff needing to have access to any website that falls under these categories must have permission form the Headteacher or Chief Executive Officer

- Access to social media will be allowed for staff and blocked for students unless directed differently by the Headteacher or the Trust Digital Strategy Lead e.g. some sixth form digital courses require students to use some aspects of social media as part of their course

- The remaining settings for each profile will be reviewed annually by the DSL and/or Trust Digital Strategy Lead to ensure that settings are appropriate and that groups of students are not over-blocked or restricted

- Google safe search will be enabled for all students and thumbnail images from websites in blocked categories will be blocked

- Where a website is blocked, staff will be able to request access via the Trust helpdesk system

- Access to a live Internet filtering dashboard and subsequent reporting will be limited to the IT technical staff, the Trust Digital Strategy Lead and any designated staff under the direction of the Headteacher or Designated Safeguarding Lead

- Internet histories are retained for a period of time (restricted by file storage space) but are available for a minimum of 30 days and are typically available for 60 days

- Internet browsing histories of students can be requested by a member of SLT

- Internet browsing histories of staff must be requested by the Headteacher or the Chief Executive Officer

- Logins for the Wi-Fi on BYOD devices will be restricted to a nominated network connection and will require central authentication through the Trust portal. The filtering for these connections will follow the same policies as for students.

- Students who deliberately take action to evade filtering restrictions e.g. by using a VPN will have their access to the BYOD Wi-Fi revoked

Key Stroke Monitoring:

- Computer usage will be monitored by Smoothwall with a key-logging agent installed on all Trust-owned computers

- Logins to the Trust Smoothwall dashboard are limited to the Chief Executive Officer and the Digital Strategy Lead

- Logins for each academy will be created for the Headteacher and designated safeguarding staff

- Automated safeguarding alerts will be as directed by the Headteacher and/or DSL and will be set up as follows:

    - Alerts for Students – the Child Protection / Safeguarding team and designated behaviour managers for each relevant year group. Alerts set at Level 3 or higher will be automatically sent to CPOMS
    - Alerts for Staff – the Headteacher, Chief Executive Officer and the Trust Digital Strategy Lead

Email:

- Email will be filtered through Clearswift Secure Email Gateway with categories of concern visible to all technicians except 'e-Safety Concern' which will only be visible to the Digital Strategy Lead and Infrastructure Admins. Email is further filtered by Microsoft with their own Phishing/Malware checks only

- Mail that is detected under the 'e-Safety Concerns' rule will trigger an automatic email to the Digital Strategy Lead and Infrastructure admins

- Whilst the filtering of the system operates continuously, staff are not expected to monitor alerts outside their normal working hours

- Student email accounts may be accessed at the discretion of a member of SLT

- Staff email accounts items may be accessed with written authorisation from the Headteacher, the Chief Executive Officer or, under certain circumstances, the member of staff themselves e.g. where a member of staff requires help in managing a folder or changing settings

Appendix B: Mobile and Smart technology

- The academy is not responsible for the loss, damage or theft of any personal device that is brought into school or used for academy or Trust business

- Any personal device brought on site, or used for academy/Trust business including, but not limited to, laptops, smart phones, tablets, cameras, games consoles, smart watches and other wearable technology falls under the requirements of the separately published guidance.

- Emerging technologies will be examined for educational benefit and (if indicated) a full Data Protection Impact Assessment (DPIA) will be carried out before use in an academy is allowed

Staff

- Staff are granted access to the academy/Trust IT equipment and services at the discretion of the Headteacher or the Chief Executive Officer

- Staff are permitted to bring personal technology on site at the discretion of the Headteacher or the Chief Executive Officer

- Staff are able to gain access to systems in advance of their contracted start date provided they have formally accepted a job offer, have successfully completed a DBS check and need access to some information prior to commencement of employment e.g. a new teacher needing access to faculty resources to plan for lessons ahead of a new term. This does not included access to personal data stores such as SIMS or CPOMs, which will not be granted until the start of the employment contract.

- Staff are expected to read the guidance regarding all devices and IT usage (published annually)

Students

- Students are granted access to the academy/Trust IT equipment and systems at the discretion of the Headteacher or the Chief Executive Officer

- Students are permitted to bring personal technology on site at the discretion of the Headteacher or the Chief Executive Officer

- Any electronic device brought into the academy may be confiscated by any member of staff if the use falls under the Unacceptable Use definition

- Any electronic device brought into the academy may be searched by an authorized staff member if they have reasonable grounds for suspecting it:
    - poses a risk to staff or pupils;
    - is prohibited, or identified by the Headteacher or the DSL as a concern
    - is evidence in relation to an offence

- Students are reminded of their responsibilities regarding online safety and the use of technology through the Student Agreement which they will sign annually to confirm understanding

- Students will receive lessons on the safe and responsible use of technology informed by the statutory guidance in the current versions of ‘Relationships Education, Relationships and Sex Education (RSE) and Health Education’ and ‘Keeping Children Safe in Education’

Parents/Carers

- Parents/carers will be made aware of the academy’s behaviour expectations regarding the acceptable/unacceptable use of technology on induction and through the academy website

- Parents/carers will be made aware of the arrangements for remote learning through the academy website

- Parents will be encouraged to support their child in their responsible use of technology through the website, events in academy and individual discussions

- Parents/carers will be offered bespoke advice in response to a digital concern

Appendix C: Curriculum

Online safety is fully embedded within our curriculum(s). The academy provides a comprehensive age-appropriate curriculum for digital safety which enables pupils to become informed, safe and responsible users of technology.

The curriculum offer is informed by the statutory guidance in ‘Relationships Education, Relationships and Sex Education (RSE) and Health Education’, ‘Keeping Children Safe in Education’ and local factors. However, the curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Whilst a whole school approach is developing, the majority of this work is delivered in citizenship, PSHE and form time activities as well as focus timetable days and the Computing curriculum.

Curriculum work includes areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives.

- Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people’s information, reputation, and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

Appendix D: Staff Training (including data protection training)

Staff are expected to undergo regular training in the areas of online safety and data protection.

On induction (of employees and trainee teachers):

- A section on esafety and data protection including recommendations for creating passwords
- Online esafety course (renewable annually)
- NCSC Cyber Security training video

On arrival (Supply/agency staff)

- Safeguarding leaflet

Annual reminders:

- IT agreements – signed
- Online safety, data protection and cyber security guidance document – signature on reading required
- Online safety reminders – in INSET training
- Online course renewal through the Child Protection Company (or similar) (annually)

Each term:

- Phishing campaign (with follow up training if needed)

Ad hoc:

- Specific software training
- In response to an incident
- In the event of an external concern
- On request
- Social Media Champions – training when new staff take on an account

Appendix E: Student Training (including data protection)

September:

- Form time reminders of expected behaviour including online
- Reminders of filtering and monitoring software and the alerts within each academy
- Reinforcements of password security
- IT agreements reviewed and signed
- Yr 7 and 12 - Lessons on familiarising themselves with the new IT systems
- Yrs 9+ asked to read Data Protection summary and grant consent for the use of their image (if they are able to make an informed decision)
- Yrs9+ emailed copy of the student Data Privacy Notice

Ongoing:

- PSHRE/Form Time lessons addressing the areas in the statutory Relationships and sex education (RSE) and health education from the DfE
- Online safety lessons incorporated in KS3 Computing curriculum
- Signposting to support agencies for online concerns available electronically and made visible/signposted in assemblies, PSHRE/Form Time activities and citizenship lessons
- Facilities for reporting concerns including online concerns available via academy websites

Ad hoc:

- Support in response to an incident
- Support in the event of an external concern
- On request

Appendix F: IT Technicians (including data protection)

By the nature of their role, IT technicians will have (or could grant themselves) access to material which is private, confidential and/or sensitive in nature. It is also likely that their role will involve testing security settings or reviewing new software and websites. In these tasks, they may need to use vocabulary which would otherwise be considered inappropriate for a workplace or may access or attempt to access websites which are deemed as unsuitable for the workplace.

Technicians will:

- respect confidentiality and privacy at all times
- only access the areas of the network or systems which are necessary for them to perform a designated task
- ensure that the monitoring and filtering systems work effectively in order that any misuse/attempted misuse is reported to the relevant person in a timely manner
- request and keep a record of any authorisations needed to access the accounts of other staff or students in light of the guidance in the other sections
- check the categories of any website before unblocking and request confirmation from the DSL, Headteacher, IT Infrastructure Engineer, Director or Trust Digital Strategy Lead where the site is not directly (and obviously) related to an educational task
- check that any requested software installation is checked against the central software register and coordinate with the Trust Digital Strategy lead where the software has not yet been accepted onto the register
- ensure that only students with written consent from at least one parent have biometric recognition enabled
- report any concerns immediately using the appropriate reporting mechanism
- keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant