E-Safety Policy

Nominated Lead Member of Staff:	**Anthony Taylor**
Date of Policy:	**June 2020**
Status & Review Cycle:	**Annual**
Next Review Date:	**June 2021**

Contents

1. What is the E-Safety Policy? 4
   1.1 Aims of the E-Safety Policy 4
   1.2 Scope of the Policy 4
   1.3 Links to Other Policies 5
2. Relevant Laws/Documentation 5
   2.1 Additional Notes 6
3. Monitoring and Responsibility 7
   3.1 Governing Body 7
   3.2 Principal 8
   3.3 E-Safety Committee 8
   3.4 Nominated Governor 9
   3.5 Personnel (Including Teaching Staff) 9
   3.6 Safeguarding Team 10
   3.7 Pupils 10
   3.8 Most Vulnerable pupils 11
   3.9 Parents/Carers 11
   3.10 Network Manager / Technical staff: 11
   3.11 Other users 12
4. E-Safety in the Curriculum 12
5. Internet Filtering and use 13
6. Authorising Internet Access 13
7. Password Security 13
8. Use of External Media 13
9. Bring your own Device (BYOD) 14
10. Mobile Phones and Devices 14
   10.1 Pupil Mobile Phone Use: 14
   10.2 Staff Mobile Phone Use: 14
   10.3 Responsibility 14
11. Cyberbullying 14
12. Email 14
13. Classification of Inappropriate Activities 15
14. Staff using Work Devices outside the Academy 15
15. Academy Website 16
16. Social Networking and Personal Publishing 16
17. Inappropriate Material 17
18. Sexting 17
19. Complaints of Internet Misuse 17
20. Children with Special Educational Needs (SEN) 17
21. Raising Awareness of this Policy 17
22. Training 17

23. Reporting Incidents 18
24. Examining Electronic Devices 18
25. Equality Impact Assessment 19
26. Monitoring the Effectiveness of this Policy 19

1. What is the E-Safety Policy?

The Academy E-Safety policy aims to create an environment where pupils, staff, parents, governors and the wider community work together to inform each other of ways to use the Internet responsibly, safely and positively. Internet technology can help pupils learn creatively and effectively. The E-Safety policy encourages appropriate and safe conduct and behaviour while achieving this. Pupils, staff and all other users of Academy related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure safe and good behaviour. These agreements and their implementation will promote positive behaviour which can impact directly on a pupil's adult life and prepare them for experiences and expectations in their futures. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to teach and inform, in order to develop positive behaviours and knowledge leading to safer Internet usage. It is intended that the positive effects of the policy will be seen online and offline; in the Academy and at home; and ultimately beyond Academy life and into the future.

1.1 Aims of the E-Safety Policy

- To provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote pupil achievement.
- To protect children from the risk of radicalisation and extremism.
- To ensure compliance with all relevant legislation connected to this policy.
- To work with other academy's and the local authority to share good practice in order to improve this policy.

1.2 Scope of the Policy

This policy applies to all members of the academy community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of academy.

The Academy E-Safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider community who use, have access to or maintain the Academy and Academy related Internet and computer systems internally and externally.

The Academy will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the Academy site. This will include imposing rewards and sanctions for behaviour and penalties for inappropriate behaviour – as defined as regulation of student behaviour under the Education and Inspections Act 2006. 'In Loco Parentis' provision under the Children Act 1989 also allows the Academy to report and act on instances of cyber bullying, abuse, harassment, malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The E-Safety policy covers the use of:

- Academy based ICT systems and equipment.
- Academy based intranet and networking.
- Academy related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, and social media websites.
- External access to internal Academy networking, such as webmail, network access, file-serving (document folders) and printing.
- Academy ICT equipment off-site, for example staff laptops, digital cameras, mobile phones.
- Pupil and staff personal ICT equipment when used in the Academy and which makes use of academy networking, file-serving or Internet facilities.
- Mobile phones, devices and laptops when used on the Academy site.

1.3 Links to Other Policies

This policy makes reference to the Acceptable Use Policy statement for both staff and pupils (AUP), which has been agreed by governors. A copy of this statement can be found in Appendix 3. It applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of academy.
The E-Safety policy should be reviewed in line with the following policies:

- Child Protection and Safeguarding Policy
- MEA Behaviour for Learning & Anti-Bullying Policy
- Social Networking Policy
- Acceptable use policy

2. Relevant Laws/Documentation

We believe this policy relates to the following **legislation**:

- Obscene Publications Act 1959
- Protection of Children Act 1978
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 1998
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003
- Sexual Offences Act 2003
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Racial and Religious Hatred Act 2006
- The Education and Inspections Act 2006 (Head teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the academy behaviour policy.)
- Children and Young Persons Act 2008
- Academy Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011

- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015

The following **documentation** is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Principals, Academy Staff, Governing Bodies and Proprietors of Independent Academys (DfE)
- Equality Act 2010: Advice for Academy's (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Academy's and Colleges (DfE)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

2.1 Additional Notes

Copyright infringement and DMCA:
If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto site such as Facebook and Twitter.

Duty of care and 'in loco parentis':
Academies have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989, this enables academies to remove personal information, cyber bullying and comments relating to academy pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all academy's, but especially to boarding and residential academy's.

Specific academy policies to support good practice in E-Safety:

Acceptable Internet Usage Policy:

- The academy Acceptable Internet Usage Policy covers use by pupils, staff and other adults working in academy and also the usage of academy related Internet technologies such as extranets, E-Learning platforms, website, social media and external network logins.
- Acceptable Use policies are tailored for each Key Stage for pupils; and by category of adult. These policies are signed annually by pupils, staff and other adults working in academy, or those with access to academy related technologies – for example external contractors responsible for the academy website or E-Learning platform.
- The purpose and scope of the E-Learning Policies are explained to those required to sign and agree to them by means of a presentation and opportunity to ask questions. New pupils will be informed of the scope and purpose of the AUPs as part of induction prior to joining the academy, or at the start of their first term. For pupils, this purpose and scope is also explained to parents by means of explanatory notes accompanying the policy to sign, and in presentations on E-Safety provided to parents at regular points in the academy E-Safety calendar.
- It is assumed that pupils and staff will not be granted access to academy Internet and related Internet technologies until the AUP agreement has been signed.
- Reciprocal agreements are designed to promote positive Internet behaviours, both at academy and at home. Such agreements are not designed to be simply a list of prohibited activities.

We believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the academy's management information and business administration systems

We acknowledge that the increased provision of the Internet in and out of academy brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

E-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the academy community have an entitlement to safe Internet access at all times.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremists groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism. Academy personnel must be aware of the increased risk of online radicalisation and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that academy personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

We wish to work closely with the Academy Council and to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy

3. Monitoring and Responsibility

The E-Safety policy will be actively monitored and evaluated by an E-Safety committee.
This committee will comprise:

- VP Safeguarding and Inclusion: P Jarvis
- Academy Digital Leader: A Taylor
- IT Infrastructure Manager: P Gartland
- Alternative Provision Lead : M Chapman
- Inclusion Strategy Leader: T Brough

3.1 Governing Body

The Governing Body has:

- appointed a member of staff to be responsible for E-Safety;
- delegated powers and responsibilities to the Principal to ensure all academy personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring that the academy complies with all equalities legislation;

- nominated a designated Equalities governor to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- make effective use of relevant research and information to improve this policy;
- responsibility for ensuring policies are made available to parents;
- undertaken training in order to understand E-Safety issues and procedures;
- nominated a link governor to visit the academy regularly, to liaise with the Principal and members of the E-Safety Committee and to report back to the Governing Body;
- responsibility for the effective implementation, monitoring and evaluation of this policy.
- Ensure new members of staff are given child protection training which includes online safety.
- At least one Governor is responsible for E-Safety and a member of the E-Safety Committee will liaise directly with the Governor with regard to reports on E-Safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider community.
- It is essential that Governors tasked with overseeing and monitoring E-Safety have demonstrable experience, skills or qualifications to match the role.

3.2 Principal

The Principal will:

- ensure the safety and E-Safety of all members of the academy community;
- ensure all academy personnel, pupils and parents are aware of and comply with this policy;
- work closely with the Governing Body and the E-Safety Committee to create a safe ICT learning environment by having in place:
  - an effective range of technological tools
  - clear roles and responsibilities
  - safe procedures
  - a comprehensive policy for pupils, staff and parents
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- embed E-Safety in all aspects of the curriculum and other academy activities;
- work closely with the link governor and E-Safety committee;
- provide leadership and vision in respect of equality;
- make effective use of relevant research and information to improve this policy;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy by:
  - monitoring learning and teaching through observing lessons
  - monitoring planning and assessment
  - speaking with pupils, academy personnel, parents and governors
- annually report to the Governing Body on the success and development of this policy.

3.3 E-Safety Committee

The committee will:

- be responsible for the day to day E-Safety issues; this is delegated by incident type.
- undertake an annual E-Safety audit in order to establish compliance with LA guidance;
- ensure that all Internet users are kept up to date with new guidance and procedures;
- have editorial responsibility of the academy website and will ensure that content is accurate and appropriate;
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- undertake risk assessments in order to reduce Internet misuse;
- maintains a log of all E-Safety incidents;
- reports all E-Safety incidents to the Principal where appropriate;
- ensure E-Safety is embedded in all aspects of the curriculum and other academy activities;

- lead the development of this policy throughout the academy;
- work closely with the Principal and the nominated governor;
- make effective use of relevant research and information to improve this policy;
- provide guidance and support to all staff;
- provide training for all staff on induction and when the need arises;
- keep up to date with new developments and resources;
- review and monitor;
- report annually to the Governing Body on the success and development of this policy.
- The Academy has a designated E-Safety lead [Anthony Taylor] who reports to the SLT and Governors and coordinates E-Safety provision across the Academy and wider community as appropriate. The committee liaises with SLT, the Academy's designated Community and Safeguarding Leader /Inclusion Leader and other senior managers as required.
- The Academy E-Safety lead has a specific job description and person specification detailing the role, remit, qualifications and qualities required for the post. This specification is updated according to the Academy cycle for reviewing job descriptions.
- The Academy E-Safety Committee meets regularly at intervals.
- The Academy E-Safety Committee is responsible for E-Safety issues on a day to day basis and also liaises with filtering and website providers and Academy ICT support.
- Although all staff are responsible for upholding the Academy E-Safety policy and safer Internet practice, the E-Safety and SMS lead, the Child Protection team and IT Infrastructure Manager: are responsible for monitoring Internet usage by pupils and staff, and on Academy machines, such as laptops, use off-site.
- The E-Safety lead will regularly update the website so relevant information is given to parents as it arises.

3.4 Nominated Governor

The Nominated Governor will:
- work closely with the Principal and the E-Safety committee;
- ensure this policy and other linked policies are up to date;
- ensure that everyone connected with the academy is aware of this policy;
- undertake appropriate training;
- report to the Governing Body every term;
- annually report to the Governing Body on the success and development of this policy

3.5 Personnel (Including Teaching Staff)

Academy personnel will:
- comply with all aspects of this policy
- undertake appropriate training;
- before using any Internet resource in academy must accept the terms of the 'Responsible Internet Use' statement;
- be responsible for promoting and supporting safe behaviours with pupils;
- promote E-Safety procedures such as showing pupils how to deal with inappropriate material;
- report any unsuitable website or material to the a member of the safeguarding team;
- will ensure that the use of Internet derived materials complies with copyright law;
- ensure E-Safety is embedded in all aspects of the curriculum and other academy activities;
- be aware of all other linked policies;
- maintain high standards of ethics and behaviour within and outside academy and not to undermine fundamental British values;
- work in partnership parents and carers keeping them up to date with their child's progress and behaviour at academy;
- implement the academy's equalities policy and schemes;
- report and deal with all incidents of discrimination;
- attend appropriate training sessions on equality;
- report any concerns they have on any aspect of the academy community

- Teaching and teaching support staff need to ensure that they are aware of the current Academy E-Safety policy, practices and associated procedures for reporting E-Safety incidents.
- Teaching and teaching support staff will be provided with E-Safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to Internet and computer use in the Academy.
- All staff need to follow the Academy's social media policy, in regard to external off site use, personal use (mindful of not bringing the Academy into disrepute), possible contractual obligations, and conduct on Internet Academy messaging or communication platforms, for example email, VLE messages and forums and the Academy website.
- All teaching staff need to rigorously monitor pupil Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the Academy site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Internet usage and suggested websites should be pre-vetted before teaching the lesson.

3.6 Safeguarding Team

- The DSL and deputies need to be trained in specific E-Safety issues. Accredited training with reference to child protection issues online is advised – for example a CEOP accredited course or a Cyber mentor course.
- The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection, this does include online safety.
- The team need to be able to differentiate which E-Safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
- Possible scenarios might include:
    - Allegations against members of staff.
    - Computer crime – for example hacking of Academy systems.
    - Allegations or evidence of 'grooming'.
    - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

3.7 Pupils

Pupils will be aware of this policy and will be taught to:

- be critically aware of the materials they read;
- validate information before accepting its accuracy;
- acknowledge the source of information used;
- use the Internet for research;
- respect copyright when using Internet material in their own work;
- report any offensive e-mail;
- report any unsuitable website or material to a member of staff;
- know and understand the academy policy on the use of:
    - mobile phones
    - digital cameras
    - hand held devices
- know and understand the academy policy on the taking and use of photographic images and cyber bullying;
- Pupils are required to use Academy Internet and computer systems in agreement with the terms specified in the Academy Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
- Pupils need to be aware of how to report E-Safety incidents in the Academy, and how to use external reporting facilities, such as the CEOP report abuse button.
- Pupils need to be aware that Academy Acceptable Use Policies cover all computer, Internet and gadget usage in the Academy, including the use of personal items such as phones.

- Pupils need to be aware that their Internet use out of the Academy on social networking sites such as Facebook is covered under the Acceptable Use Policy if it impacts on the Academy and/or its staff and pupils in terms of cyber bullying, reputation or illegal activities.

3.8 Most Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, for example Looked After Children and those with Special Educational Needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online.

Staff must be aware that vulnerable pupils need more support and will be responsible for providing this through their role.
Information on how to do so can be found from:

- Vulnerable Children in a Digital World - Internet Matters
- Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group STAR SEN Toolkit - Childnet

3.9 Parents/Carers

Parents/carers will:
- be aware of and comply with this policy;
- be asked to support the E-Safety policy and to sign the consent form allowing their child to have Internet access;
- make their children aware of the E-Safety policy;
- It is hoped that parents and guardians will support the Academy's stance on promoting safe Internet behaviour and responsible use of IT equipment both in the Academy and at home.
- The Academy expects parents and guardians to sign the Acceptable Use Polices , indicating agreement regarding their child's use and also their own use with regard to parental access to Academy systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.
- The Academy will provide opportunities to educate parents with regard to E-Safety.

3.10 Network Manager / Technical staff:

The Network Manager is responsible for ensuring:
- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required E-Safety technical requirements and any Local Authority / other relevant body E-Safety Policy that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the network / Internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; E-Safety Committee
- that monitoring software / systems are implemented and updated as agreed in academy policies
- internal ICT support staff and technicians are responsible for maintaining the Academy's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the Academy system, particularly file-sharing and access to the Internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.

- support staff also need to maintain and enforce the Academy's password policy and monitor and maintain the Internet filtering.
- external contractors, such as VLE providers, website designers/hosts/maintenance contractors should be made fully aware of and agree to the Academy's E-Safety Policy. Where contractors have access to sensitive Academy information and material covered by the Data Protection Act, for example on a VLE, Academy website or email provision, the contractor should also be CRB checked.

3.11 Other users

- Other users such as visitors, wider community stakeholders or external contractors should be expected to agree to a visitor's AUP document or a tailored AUP document specific to their level of access and usage.
- External users with significant access to Academy systems including sensitive information or information held securely under the Data Protection Act should be CRB checked. This includes external contractors who might maintain the Academy domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

4. E-Safety in the Curriculum

Staff will be made aware of the DfE advice outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements which can be found at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
• **content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
• **contact**: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

From September 2020, Relationships Education will be compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England.

The e-safety curriculum:

- will complement the computing and fantastic futures curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- will include guidance only the following;
    - how children evaluate what they see online
    - persuasion techniques
    - online behavior
    - online harms and risks
    - privacy and security
    - how and when to seek support
    - Copyright and ownership
    - Disinformation
    - Social engineering
    - Mental health and wellbeing

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology
- ensures pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments and are considerate of appropriate content

5. Internet Filtering and use

We have a contract with a reputed and national Internet provider to manage a secure and filtered internet service which enables us to safely access and use the Internet and all email. The internet filtering service will be annually reviewed.

Access to the internet is designed to protect pupils and academy personnel by blocking the following content:

- adult content containing sexually explicit images
- violent content containing graphically violent images
- hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs
- criminal content relating to the promotion of criminal and other activities
- gambling content relating to the use of online gambling websites
- non-educational websites such as social networking sites

All users access the Internet in accordance with the Academy's Acceptable Internet Use & Agreement and will inform the IT Network Manager if at any time they find they have accessed inappropriate internet sites.

When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary the Police.

6. Authorising Internet Access

- Before using any academy ICT resource, all pupils and staff must read and sign the 'Acceptable ICT Use Agreement'.
- Parents must sign a consent form before their child has access to the Internet.
- An up to date record will be kept of all pupils and academy personnel who have Internet access.

7. Password Security

All users are responsible for the security of their username and password and must not allow other users to use this information to access the system. All breaches of security must be reported.

8. Use of External Media

All academy staff, of any description outlined in this policy, should be aware of how to store and share/send electronic data. Staff should not use external media to save information, directly or indirectly, associated with the academy, without sufficient encryption and data encryption. Staff should also consider the following:

- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)

- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

If staff are in any doubt of this they should see the network manager or E-Safety leader in the first instance, before using external media.

9. Bring your own Device (BYOD)

The academy has not yet implemented a BYOD policy. If devices are to be used on site they must be first approved by the network manager. It is understood that the academy is not liable for the security of **personal** devices.

10. Mobile Phones and Devices

10.1 Pupil Mobile Phone Use:

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:
• they can make students and staff more vulnerable to cyberbullying
• they can be used to access inappropriate Internet material
• they can be a distraction in the classroom
• they are valuable items that could be stolen, damaged, or lost
• they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The academy therefore adopts a zero tolerance Electronic Device Policy for students during the academy day, except at break times. Phones and electronic devices (including headphones) can be confiscated. Any student who refuses to hand over the complete phone (battery and SIM card) / device when requested will be removed from the lesson and their behaviour will be considered as defiant. The academy's BfL policy will then be followed.

10.2 Staff Mobile Phone Use:

Under no circumstances should staff use their own personal devices to contact students or parents either in or out of academy time unless in an emergency. Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the academy curriculum or for a professional capacity, the academy equipment will be used for this.

10.3 Responsibility

The academy accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in/confiscated. The academy will not investigate theft, loss or damage relating to phones/devices.

11. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the academy. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the anti-bullying policy. Please refer to this document in how the academy classifies cyberbullying and deals with incidents.

12. Email

Pupils must:
- only use approved e-mail accounts;
- report receiving any offensive e-mails;
- not divulge their or others personal details;

- not arrange to meet anyone via the e-mail;
- seek authorisation to send a formal e-mail to an external organisation
- not take part in sending chain letters

13. Classification of Inappropriate Activities

Some Internet activity e.g. accessing child abuse images or disturbing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the user or the nature of those activities.
The academy believes that these activities would be inappropriate in our academy context:
• pornography
• promotion of any kind of discrimination
• threatening behaviour, including promotion of physical violence or mental harm
• any other information which may be offensive to anyone in the academy community or breaches the integrity of the ethos of the academy or brings the academy into disrepute
• using academy systems to run a private business
• using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy
• infringing copyright
• revealing or publicising confidential or proprietary information e.g. financial, personal information, databases, computer / network access codes and passwords
• creating or propagating computer viruses or other harmful files
• unfair usage
• on-line gaming, educational and non-educational
• on-line gambling
• use of social media without permission
• use of messaging apps without permission
• use of videoing broadcasting or YouTube without permission

14. Staff using Work Devices outside the Academy

Staff Devices
Staff members using a work device outside academy must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside academy. Any USB devices containing data relating to the academy must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
Work devices must be used solely for work activities.

Distance Learning and Remote Working
Due to the change in working circumstances caused by Covid-19, Manchester Enterprise Academy have adapted the use of Microsoft Teams, amongst other software, to aid distanced working and learning. Any member of staff which uses any software or website to communicate with staff or students must be adhere to the points below:

- **Wear appropriate clothing.** Be aware that laptop cameras give different and sometimes unexpected camera angles, therefore wear what you would wear if you were in school.
- **Don't go online from your bedroom**. Be aware of the background you are projecting. Are there any photographs etc. you wouldn't want students to see? You are welcome to conduct your live lesson from school.

- **Warn others in your house when you are broadcasting online.** Family members should not be visible on camera.
- **Always record your session**. This will protect you from any form of allegation. Sessions once recorded are automatically uploaded on the Team chat.
- **Ensure that two members of staff are present on all live lessons**. The second staff member may be in the 'background' solely as an observer and have their video turned off.
- **Avoid 1:1 support.** If pupils require additional support, email them and copy in your Head of Faculty / line manager.
- **Use the chat function appropriately.** Some students may which to use the chat function. This must be conducted in a formal manner. If you receive an inappropriate message, forward this to your line manager, a member of the e-safety team. If it poses a safeguarding issue also log the incident on CPOMS, with a screen shot, and alert a member of the Safeguarding Team.
- **Only** use approved methods of online communication, in this case Microsoft Teams and your Academy email address.
- **Do not** use any form of social media to engage pupils in their online learning.
- **Think about your use of language.** Not using inappropriate language goes without saying but be aware that our students may well be worried or anxious at this time. Keep calm, re-iterate the government message of washing hands and social distancing.
- **Consider the safeguarding of each child you teach online.** You may be the only non-family member they are going to see that day. Listen for any cues that indicate a safeguarding concern and report these to a member of the Safeguarding Team as soon as possible. These cues may indicate, but may not be limited to:
    - Child abuse or neglect
    - Inadequate supervision at home
    - The impact of food poverty
    - The health status in a family and any young carer responsibilities they are having to pick up.
    - Domestic violence

15. Academy Website

Contact details on the website will be:

- the academy address
- e-mail address
- telephone number

The academy website will not publish:

- staff or pupils personal contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

16. Social Networking and Personal Publishing

Pupils will not be allowed access:

- to social networking sites except those that are part of an educational network or approved Learning Platform;
- to newsgroups unless an identified need has been approved

Academy staff should ensure that:

- No reference is made in social media to students / pupils, parents / carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the academy or local authority

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The academy's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety Committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

17. Inappropriate Material

Any inappropriate websites or material found by pupils or academy personnel will be reported to the Network Manager or E-Safety Lead who in turn will report to the Internet Service Provider.

18. Sexting

All incidents of sexting, including new procedures in relation to up-skirting, will be dealt with by:

- meeting with the appropriate Academy personnel;
- meeting with the pupils involved;
- informing the parents unless by doing so will put the pupil(s) at risk;
- not viewing the imagery unless it is unavoidable;
- contacting social care or the police if the pupil is at risk of harm.
- To make Academy personnel aware of the increased number of cases of sexting among under 16 year olds and the damaging effects that it is having.
- To ensure sexting becomes an important topic for discussion with students as part of the Fantastic Futures curriculum.
- Contacting a relevant member of the Safeguarding Team (P Jarvis / T Brough / M Chapman).

19. Complaints of Internet Misuse

- The Principal will deal with all complaints of Internet misuse by academy personnel.
- The Safeguarding Team or Network Manager will deal with all complaints of Internet misuse by pupils. Internet Misuse must be reported to a relevant member of staff.
- Parents will be informed if their child has misused the Internet.

20. Children with Special Educational Needs (SEN)

Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. These risks include, but are not limited to; online bullying, grooming and radicalisation. The SENCO is responsible for ensuring heath care plans consider this.

21. Raising Awareness of this Policy

We will raise awareness of this policy via:

- the academy website
- the Staff Handbook
- meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- academy events
- meetings with academy personnel
- communications with home such as weekly newsletters and of end of half term newsletters
- reports such annual report to parents and Principal reports to the Governing Body
- information displays in the main academy entrance
- staff inset and training, where necessary

22. Training

All academy personnel, including governors:

- have equal chances of training, career development and promotion
- receive training/assistance which specifically covers:
  - All aspects of this policy
  - Safeguarding & Child Protection
  - Anti - Cyber bullying
  - Acceptable Internet Use Agreement
  - ICT
  - Pupil Behaviour & Discipline
  - Anti-bullying
  - Academy Website
  - Mobile Phone Safety & Acceptable Use
  - Photographic & Video Images
  - Internet Social Networking Websites
  - Equal opportunities
  - Inclusion
- receive periodic training so that they are kept up to date with new information
- will refer to Schools can refer to the Education for a Connected World Framework for age specific advice about the online knowledge and skills that pupils should have
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications.

23. Reporting Incidents

In the event of an E-Safety incident of any type, it is important that the correct member of staff is notified immediately. If the incident is of a safeguarding or child protection nature [regarding a pupil], a member of the Safeguarding Team (M Chapman / T Brough / P Jarvis) must be notified. If the incident is not then the student's pastoral manager, the P Gartland and A Taylor must be notified. If the incident is concerning a staff member the Principal must be notified. Incidents which involve the safety or concern of a child must be logged on CPOMS as soon as possible.

24. Examining Electronic Devices

Academy 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 pupils' 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
- Disrupt teaching, and/or
- Break any of the academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with a member of the Senior Leadership Team (SLT) to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of academy discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the academy complaints procedure. This is detailed in the academy's complaints and grievances policy.

25. Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this academy.

26. Monitoring the Effectiveness of this Policy

The practical application of this policy will be reviewed annually or when the need arises by the academy's digital leader, the Principal and the nominated governor.

A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the Governing Body for further discussion and endorsement.

The E-Safety policy will be reviewed and evaluated promptly in the light of serious E-Safety incidents.

The E-Safety policy will be reviewed and evaluated promptly in the light of important changes to legislation or government guidance related to E-Safety.

The Governing Body will receive a report on the progress, evaluation, impact and effectiveness of the E-Safety policy annually. This report will include suitably redacted accounts and statistics of E-Safety incidents and how these have been resolved, and counter measures implemented.