Document Title	**MLT E-Safety Policy**
Author/Owner (Name and Title)	Director of ICT
Version Number	V2
Date Approved	10 October 2022
Approved By	MLT Board

Policy Category	**1**	**Trust/Academies to use without amendment**
	2	Academy specific appendices
(Please Indicate)	**3**	Academy personalisation required (in highlighted fields)

Summary of Changes from Previous Version

Version	Date	Author	Note/Summary of Revisions
V2	June 2022	JHE	Complete re-write.

CONTENTS

1.INTRODUCTION

Children today are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks surrounding online safety.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: child on child abuse, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.)
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

While restrictions can be placed on Academy/Trust technologies, it has to be recognised that the majority of students will have consistent access to unfiltered Internet and social media through the use of mobile technologies. A programme of awareness and education around online risk is therefore critical.

Maltby Learning Trust wants to equip children and young people with the knowledge and understanding needed to make the best use of the internet and technology in a safe, considered, and respectful way, so they can reap the benefits of the online world and go on to lead successful and fulfilling lives.

LINKED POLICIES

E-Safety is associated to many different areas and therefore links to other policies including:

- MLT Child Protection and Safeguarding Policy
- MLT Safe Use of ICT Policy
- MLT Backup and Disaster Recovery Policy
- MLT Data Protection Policy
- MLT Anti Bullying Policy
- MLT Social Media Guidance
- MLT Behaviour Policy

REVIEW

The E-Safety policy is regularly benchmarked across the Trust using frameworks such as 360 Safe.

It is reviewed annually and updated in line with developments in technology and practice with input from all stakeholders.

2. ROLES AND RESPONSIBILITIES

Role	Key Responsibilities
Board of Trustees	• Ensuring that this policy and associated practices are embedded across the Trust. • Overall responsibility for e-safety provision. • Overall responsibility for data and data security (SIRO).
Academy Principal and Local Governance committee	• Ensure that appropriate policies linked to e-Safety are in place including Safeguarding, Safe Use of ICT and Behaviour policies. • Ensure that appropriate Internet filtering, monitoring and alert systems are in place at the Academy, and to work with ICT support to ensure the safety and security of networks. • Ensure a progressive age-related e-Safety curriculum is embedded at the Academy that promotes digital literacy, resilience, and responsibility. • Support the DSL/e-Safety co-ordinator by ensuring they have the resources and time to allow them to fulfil their obligation to e-Safety. • Establish procedures for the monitoring and reporting of E-Safety incidents and inappropriate internet use, by either students or staff. • Be aware of the procedures to follow in the event of an E-Safety incident.
Designated Safeguarding Lead (DSL)	The Designated Safeguarding Lead (DSL) has lead responsibility for e-Safety. This role may be delegated to an appropriately trained member of staff acting as e-Safety co-ordinator and/or DDSL. • Promote an awareness and commitment to e-Safety throughout the school community. • Keep up to date with e-Safety issues and legislation and communicate this with stakeholders as necessary. • Perform an annual review of e-Safety related practice at the Academy in line with a recognised framework i.e., 360 review. • Ensure all staff receive regular and appropriate e-Safety training. • Ensure that e-Safety is embedded across the curriculum. • Liaise with Academy/Trust technical staff. • Ensure that all staff are aware of the procedures to follow in the event of an E-Safety incident. • Log incidents and review, using this data to update current policy and practice where appropriate. • Communicate regularly with SLT and Governors to discuss current issues and review incident logs.
ICT Support	• Provide technical support to the DSL to ensure the implementation and maintenance of e-Safety policy and procedure. • Maintain and update the Academies/Trust Internet filters and reporting mechanisms and follow procedures for change control. • Ensure IT systems are secure and not open to misuse or attack. • Report any e-Safety related issues to the DSL.
All Staff	• Ensure that students are protected and supported in their use of on-line and off-line technologies so that they know how to use them in a safe and responsible manner, they can be in control, and they know what to do in the event of an incident. • Be able to identify an e-Safety incident and know how to react. • Model good practice when using technology and maintain a professional level of conduct, including personal use, both on and off site. • Ensure their e-Safety knowledge is current and embed this knowledge through curriculum delivery where possible. • Adhere to the Academy/Trust ICT Acceptable Use agreement.
Staffs	• Understand the importance of always adopting good e-Safety practice when using digital technologies. • Play an active part in the development of the e-Safety policy.

	• Adhere to the Academy/Trust policy on the use of personal mobile devices. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • Know how to, and have the confidence to, report any inappropriate materials or contact from someone they do not know immediately, without fear of reprimand.
Parents/Carer	• Read the ICT acceptable use agreement and encourage their children to adhere to it. • Re-enforce good e-Safety practice for the young people in their care, outside of the school day. • Role model the safe use of ICT and social media. • Be aware of any changes in behaviour that could indicate their child is at risk of harm online. • Seek help from the Academy or other agencies if their child encounters risk online.

3. REDUCING ONLINE RISKS

STUDENTS

An e-Safety programme will be taught across the curriculum, ensuring students are aware of the safe use of new technology both inside and outside of school. This curriculum progresses with students as they grow and develop. Current curriculums ensure learning outcomes as defined in the 2020 UKCIS framework 'Education for a Connected World 2020'.

This framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

Categories include:

1. Self-image and identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing, and lifestyle
7. Privacy and Security
8. Copyright and ownership

The use of external support where appropriate, will complement education approaches.

Clear guidance regarding the safe use of technology will be displayed around the Academy as part of ICT acceptable use agreements.

The positive use of technology by students will be recognised and rewarded.

VULNERABLE STUDENTS

Any student can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage, and personal circumstance. However, there are some students, 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.

Academies will consider how they tailor their offer to ensure these students receive the information and support they need.

STAFF

- All staff, including the Local Governance Committee, teaching and associate professionals will have access to role appropriate e-Safety training and information on a regular basis to ensure they are aware of current e-Safety issues and any changes to the provision of e-Safety.
- New staff will undergo Safeguarding training in line with the Academy/Trust induction policy.
- Staff should read and understand this policy and know how to identify and report e-Safety incidents.
- Staff should be aware that their online conduct outside of the Academy setting, including personal use of social media, could have an impact on their professional role and reputation.

PARENTS/CARERS

- The Academy will build a partnership approach to e-Safety with parents/carers, communicating through social media and workshops, updates on current E-Safety issues and promoting confidence regarding the safe use of ICT.
- Parents/carers should be aware of the various channels available via the Academy, or externally, for reporting e-Safety incidents.

4. INTERNET FILTERING

All staff and students have access to the Internet on site, accessed either through Wi-fi or via network joined devices, using their Academy/Trust login.

- ICT Support are responsible for maintaining Internet filtering solutions across the Academy/Trust.
- Internet filtering levels are age-appropriate set at each key stage. All usage is logged against user's network accounts.
- Filter categories for each key stage are agreed upon with input from curriculum and e-Safety leads.
- Mobile devices loaned to students or staff for use away from Academy/Trust sites have remote filtering enabled that uses the same categories of filtering as onsite.
- Staff may request sites to be blocked based on inappropriate content. This should be reported to ICT Support through the service desk, who will action immediately.
- There may be occasions where websites are unnecessarily blocked. Staff may request a website be unblocked by submitting a request to ICT Support via the service desk. ICT Support will check the site and unblock if appropriate.

5. MONITORING, REPORTS AND ALERTS

- Users should be aware that Internet access is filtered and monitored to protect users and the network from malicious or inappropriate content.
- Reports on Internet usage and key categories are automatically produced daily and emailed to the e-Safety lead at the Academy.
- Alerts are set for agreed categories/key words. These trigger an immediate email to the Safeguarding team.
- Incidents are regularly reviewed at E-Safety meetings and reported to the Principal and governors. This data will help inform future changes to e-Safety policy.

6. USE OF MOBILE DEVICES

The use of mobile devices is outlined within the Academy/Trust Behaviour Policy.

7. WHERE TO GET HELP

STUDENTS

- Students are encouraged to report any concerns regarding their online safety to a member of the Safeguarding team or indeed, any trusted adult.
- Concerns can also be reported via an online form found in the Safeguarding section of each Academies website.
- The Academy websites lists links to several external agencies that offer a variety of advice and support, details of these are listed in this policy. (Appendix B).

8. RESPONDING TO AN E-SAFETY INCIDENT

No two E-Safety incidents will be exactly the same and should therefore be dealt with and judged on their own merits.

INCIDENTS INVOLVING STUDENTS

Incidents should be logged and the flowchart for managing incidents should be followed (see Appendix B).

- Incidents relating to child protection are dealt with by the DSL in accordance with academy and local authority procedures. This type of incident could include for example:
    - Online sexual violence and sexual harassment – non-consensual sharing of sexual images and video, sexualised online bullying, unwanted sexual comments on social media.
    - Sharing of nudes/semi nudes.
    - Online radicalisation and extremism.

- Incidents of cyberbullying are dealt with in accordance with the Academy/Trust Anti-Bullying and Behaviour policies.

For less serious incidents* it may not be necessary to report to the DSL.

- If you do not want to approach the user or are unsure of the seriousness of the incident, you should report it to a senior member of staff who will progress the matter as appropriate.
- If you witness or are informed of anyone acting inappropriately, you should politely remind them of this e-Safety policy and of the ICT Acceptable Use Agreement (AUA), displayed in all ICT areas, to which they have agreed.
- Where students have breached the conditions of the ICT AUA, the matter may be reported to the parent/carer depending upon the seriousness of the incident.

(*) Less serious incidents may include a user being heavy handed with ICT equipment, volume of equipment being too loud, disruptive, or loud behaviour, spilled food or liquid damaging equipment, etc.

INCIDENTS INVOLVING STAFF

- Incidents involving staff should be reported to the Academy Principal or Chief Executive Officer.
- Appropriate action will then be taken in line with Child Protection and Safeguarding procedures.

APPENDIX A – CONTACTS

ACADEMY CONTACTS

Refer to each Academies Child Protection and Safeguarding Policy.

LOCAL AUTHORITY

Rotherham - Multi Agency Safeguarding Hub	(MASH)	01709 336080
Doncaster - One Front Door		01302 796191

EXTERNAL

South Yorkshire Police	999 Emergency 101 non-Emergency
Child Exploitation and Online Protection Centre (CEOP)	0207 979 5835 http://ceop.police.uk
Childline	0800 1111 http://www.childline.org.uk
Childnet – Advice for parents and carers.	https://www.childnet.com/parents-and-carers/
Digizen - Information for educators, parents, carers, and young people.	http://www.digizen.org
NSPCC – Keeping safe online.	https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Get Safe Online – Top tips for a switched-on parent.	Kids Online - Get Safe Online

APPENDIX B