MALTBYLEARNINGTRUST
Exceptional Experiences. Successful Lives.

Document Title	**MLT Safe Use of ICT Policy**
Author/Owner (Name and Title)	Director of ICT
Version Number	V2.1
Date Approved	7th June 2022
Approved By	Chief Executive Officer

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

Summary of Changes from Previous Version

Version	Date	Author	Note/Summary of Revisions
V2	January 2022	JHE	Complete re-write
V2.1	June 2022	JHE	

1.0 INTRODUCTION

STATEMENT OF INTENT

Maltby Learning Trust (MLT) believes that the safe and correct use of ICT can greatly help facilitate its vision of delivering exceptional learning experiences.

This policy outlines Maltby Learning Trust's commitment to protecting the interests and safety of all its users of ICT and related technologies.

Linked Documents

- MLT Data Protection Policy
- MLT E-Safety Policy
- MLT Remote Learning Guidance
- MLT Guidance on the Use of Social Media Accounts

SCOPE

This policy applies to the whole Trust ICT resource, including but not restricted to:

- Fixed and mobile devices including, PC's, laptops, tablets, phones.
- Interactive screens and projectors.
- Digital video recorders and cameras.
- Peripherals such as keyboards, mice and monitors.
- Telephony services.
- Televisions and media players.

This policy also applies to any software and online services provided by the Trust to aid learning and/or administration functions.

2.0 ROLES AND RESPONSIBILITIES

Role	Key Responsibilities
Trust Leaders	• 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).
ICT Support Teams	• Keep up to date with technical developments and guidance to ensure they can effectively protect the ICT infrastructure. • Actively monitor systems for malicious activity. • Ensure that software versions on key hardware are patched and up to date. • Ensure that password policies are in place and enforced for Academy/Trust systems. • Ensure that protection is in place against malicious software (malware, anti-virus etc.) following DFE guidance. • Ensure that access control and encryption exists, to protect personal and sensitive information held on Academy/Trust devices. • Maintain and update the Academy/Trust internet filters and firewalls and follow procedures for change control. • Ensure that appropriate backup procedures exists so that critical systems and data can be recovered in the event of a disaster.
Staff Users	• Be familiar with this and any linked policies and demonstrate this through practice when using ICT. • Sign an Acceptable Use Agreement (AUA) to demonstrate their understanding of this policy. • Participate in e-safety training. • 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, be in control, and know what to do in the event of an incident. • Use ICT in an appropriate way that does not breach the General Data Protection Regulations 2018 (GDPR) and other relevant legislation.
Student Users	• Read understand and adhere to the ICT AUA. • Understand the importance of adopting good E-safety practice when using digital technologies. • 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.
Parent/Carer Users	• Parent/carers can play a vital role in supporting this policy. Discuss the student ICT AUA together so that it is clear the rules are accepted by the student with the support of the parent. • Access Academy/Trust systems in accordance with the relevant Academy/Trust AUA.
Visitors and Guest users	• Sign an acceptable use agreement prior to using any Trust ICT equipment or internet access.

3. ACCEPTABLE USE AGREEMENT (AUA)

- Acceptable Use Agreements (AUAs) are an important way of encouraging all members of the school community to take responsibility for their own safety when using technology. Effective AUAs can help to establish and reinforce safe and responsible on-line behaviours both in the Academy and in the home where many incidents of inappropriate behaviour may go undetected.
- Staff signify their understanding and acceptance of this policy by signing an AUA. Indication of this is then recorded in their staff record.

- All domain devices across the Academy/Trust display a message asking users to confirm their acceptance of the AUA before logging on (see appendix 1-5).
- Posters displaying the student AUA and key e-safety messages are displayed in prominent locations in the vicinity of ICT environments across the Academy/Trust. Its content is actively reinforced with students.

4.0 AUTHORISED USE OF THE ICT FACILITIES

ICT Facilities provided by the Academy/Trust should only be used by authorised users as required for Academy/Trust administration or educational use.

While MLT respects the privacy of users, they should be aware that any content created on Academy/Trust systems, remains the property of MLT.

Access to staff accounts by ICT Support is with approval from the account holder. However, if there is a requirement to investigate breach of this policy or, in the event of prolonged staff absence, the Chief Executive Officer (CEO), Academy Principal or Executive leader can provide the necessary authorisation for line managers to access accounts.

In extreme circumstances, should there be an immediate requirement to protect the network, ICT Support reserve the right to:

- View any/all contents of file storage areas.
- View/access transactions across the network.
- View e-mails sent and perform message traces.
- Remove access to ICT services.

5.0 UNAUTHORISED USE OF THE ICT FACILITIES

It is not permitted under any circumstance to:

- Use Trust ICT facilities for commercial or financial gain without the explicit written authorisation of the CEO.
- Physically damage the ICT facilities.
- Re-locate, take offsite or otherwise interfere with the ICT facilities without authorisation from ICT Support.
- Install hardware or software without the consent of the IT Support Team or the CEO.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the Academy/Trust's computers. This is illegal under the Computer Misuse Act.
- Purchase any ICT facilities without the consent of the IT Support team or the CEO. This is in addition to any purchasing arrangements outlined in the Trust's financial policies.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the CEO. This is in addition to any purchasing arrangement followed according to Trust policy.
- Knowingly distribute or introduce a virus or harmful code onto the Academy/Trust's networks or computers. Doing so may result in disciplinary action, including summary dismissal.
- Copy, download or distribute any material from the internet or e-mail that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission, or if the permission cannot be obtained, do not attempt to download or distribute the material.
- Use or attempt to use the Academy/Trust's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not.

- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the Trust, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Deliberately delete or destroy another's data. This is a serious infringement and will be sanctioned accordingly.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.

6.0 ACCOUNT SECURITY

Maltby Learning Trust loans accounts to allow users access to ICT resources.
Users are responsible for the security of their own account.

7.0 PASSWORDS

- Users should only use their own username and password to log onto a computer and should never disclose their password to anyone else. If you suspect that somebody else knows your password, you should change it immediately by contacting ICT Support.
- Office 365 single sign on is in place where possible to authorise access to 3rd party software.
- Passwords are not to be stored in written form.
- There may be occasions where shared accounts are used in Academies, for example Cover teacher accounts. Usage of these accounts should always be traceable to an individual user and passwords resent frequently.
- Devices should be logged off properly after use or locked if left for any period, reducing the possibility of somebody else using your account.
- Users should avoid picking obvious passwords such as those based on easily obtainable information like the name of a favourite pet.
- Users should not choose common passwords, for example '1234', 'password', 'Letmein!'. Where possible, systems are in place to prevent these passwords from being used.
- Users should not use the same password anywhere else at work or home.

8.0 MULTI-FACTOR AUTHENTICATION (MFA)

- Multi Factor Authentication (MFA) is in place and enforced for key systems across Trust including Office 365 accounts, remote access and CPOMS access.
- Users should select at least two second authentication methods for redundancy.
- Accounts with administrative access are set to require two additional authentications before remote access is granted.

9.0 PHISHING

- Phishing is the fraudulent practice of sending emails purporting to be from reputable companies or somebody you know, in order to gain access to sensitive information such as passwords or financial details etc.
- The Trust uses anti-phishing software embedded in its Office 365 tenancies. Emails detected as phishing are deleted and cases logged for administrators to view. Although the software detects 95% of phishing attempts, users should always remain vigilant and report any suspicious emails to ICT Support. Never follow a link or download an attachment in an email if you are in any doubt of its authenticity.
- The following could be signs of a phishing attempt:

    - The email has poor spelling or grammar.
    - An unfamiliar tone or greeting.

- Threats or a sense of urgency.
- Suspicious attachments.
- Inconsistencies in Email Addresses, Links & Domain Names.
- Request for credentials.

10.0 USE OF THE INTERNET AND ONLINE SERVICES

- Internet access provided by the MLT is for Trust administration and educational use only.
- The use of any Academy/Trust internet connection is monitored and logged. This includes when using personal devices (Bring Your Own Devices (BYOD)). These logs can be made available on request to the Trust CEO.
- Users must not browse, upload, or download any of the following:

    - Any material that is illegal.
    - Any copyright materials including music tracks or videos.
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations.
    - Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
    - Online gambling.
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false.
    - Any sexually explicit content.
    - Any unauthorised software.

- Web filtering is in place to protect users from malicious websites. Block categories are updated daily. Occasionally, users may want to access sites that have been category blocked by filtering solutions. Staff members may submit a change request for a site to be unblocked to ICT Support who will then check the site and action the request appropriately.
- All users should be aware that connections considered secure (SSL) are also inspected by web filters and usage logged.
- Users must not attempt to bypass filtered Internet connections while working on Trust sites, using for example personal hotspots on mobile devices.
- Only online services authorised for use by ICT Support are to be used. This is particularly important where any sign up is required and/or the sharing of personal data may take place. ICT Support can check services for GDPR compliance, authorise their use and update privacy notices should this be required.

11.0 COMMUNICATION

- Only the Academy/Trust's approved communications platforms, including e-mail, forums, blogs, chats, telephony and social media platforms, should be used for Trust business or educational use.
- MLT communication systems must not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- Users should be aware that any e-mail sent to external organisations must be written carefully and professionally.
- Members of staff should use Trust branding when sending emails. This is to include Trust provided personalised banners and correct font selection etc.
- The automatic forwarding of e-mail to domains outside the Trust is prohibited and has been disabled at Tenancy level.
- MLT communication systems should not be used with the intent to harass or bully.

- Staff who feel that they have cause for complaint as a result of a communication should raise the matter initially with their line manager or Academy Principal. If necessary, the complaint can then be raised through the MLT grievance procedures.
- Any instance of the Trust or its Academies been brought into disrepute through staff communications, may constitute misconduct and be subject to disciplinary action.

12.0 E-SAFETY

Reference is made to MLTs e-safety policy:

- Users are advised to be critically aware of the content they receive online and its source. Content should not be automatically assumed accurate.
- Users are reminded to avoid giving out personal data online that may identify them or their location.
- Students should never meet with anyone whom they contact online without specific permission from a parent, carer, or member of staff.
- Staff and students are advised to maintain profiles on social media sites at maximum privacy and deny access to unknown individuals.
- Users should avoid posting images of themselves (or hidden data within images) publicly online and consider the appropriateness of any such images knowing that retrieving them can be difficult.

Students should report any e-safety incident, or aspect of harassment or cyber-bullying, to any member of staff or Academy e-safety co-ordinator/safeguarding leads.

13.0 SOCIAL NETWORKING

Specific social media accounts have been created across the Trust on a variety of platforms for the purpose of sharing information and news.

- Only specified Academy/Trust social media accounts should be used by authorised members of staff for Trust business. Any unofficial accounts found should be reported to the Trust where their removal will be requested.
- Guidance is available as a separate document regarding the use of Trust social media accounts.
- MLT does not discourage the use of personal social media by staff and students in their own time. However, users should be aware of the following:

    - Any online harassment, bullying or serious misuse involving members of the Trust community will be dealt with in line with Trust policy.
    - Staff should not accept friend requests, or invite to be friends on social media sites, any current or past student under the age of 18 other than a close family member i.e. son/daughter.

- Under no circumstance should staff communicate with students or parent/carers via social media accounts.

14.0 SAFE USE OF IMAGES

The Trust understands that recording images of identifiable individuals constitutes as processing personal data and as such it is done in line with data protection principles.

- Student and staff photographs are held electronically in management information systems for identification purposes. These images are not to be used for other purposes unless consent is obtained.

- Parents/carers may provide consent for the use of student's images for use in display and promotional work, including online content such as website and social media channels. This consent must be specifically implied and recorded electronically in management information systems. It can be removed at any time.
- Images/video captured by individuals for recreational/personal use, are exempt from the GDPR. To respect everyone's privacy and in some cases protection, these images should not be published or made available online, nor should individuals comment on any activities involving other students in the images.
- Students should not take, use, publish, distribute, or reuse any images of others without their consent.
- Staff and students are not permitted to use personal digital equipment, such as mobile phones or cameras, to record images of students or staff. This includes when on field or residential trips.
- Students' full names should not be posted anywhere online in direct association with their image.

Staff are reminded to check SIMS each time they wish to use an image of a student to ensure the appropriate consent to use that image is in place. This includes for use in social media, websites, publications, displays in school etc.

15.0 DATA PROTECTION

Users are required to be familiar with the requirements of the General Data Protection Regulation (GDPR), and to ensure that they operate in accordance with the requirements of the Regulation.

For additional guidance, please refer to the MLT Data Protection Policy.

16.0 WORKING REMOTELY

- Working remotely refers to any work done at home, or in some place other than Academy/Trust sites. This includes accessing, storing, processing or discussing Academy information.
- All users of Maltby Learning Trust's ICT systems, equipment and data have a personal responsibility to protect information and assets that are under their control. This includes keeping them physically safe when in transit and securely storing all papers and portable ICT equipment when work is finished.
- Any member of staff allowing remote access to an unauthorised person, deliberately or inadvertently, may be subject to disciplinary proceedings.
- When working remotely, choose a sensible location, for example one that is not overlooked. Do not work on sensitive matters in a public place.
- When working from home, where possible, use a room where the door can be closed. It is the personal responsibility of the individual to make sure information is safe and the individual's household understands the need for the security measures to be taken.
- When accessing work on a personal device, for example via Office 365, documents can be worked on online and should not be downloaded to the device, therefore reducing the risk off data loss. Complexed passwords should be used to access these devices, and where possible, data encrypted. Information classed as Protected, Restricted and Confidential should not be emailed home and saved on personal devices.
- You must only remove Academy/Trust documents and equipment from the workplace where there is a business need to do so and they should be returned as soon as possible.
- When you remove equipment or documents from any site across the Trust, you are responsible for ensuring its safe transit and storage.
- When no longer required, documents containing personal data must be returned to the Academy/Trust and disposed of via the confidential waste destruction system.
- Loss of equipment must be reported to the ICT Support Team immediately. All thefts/losses of equipment will be reported to the police.

- Any loss of personal data will be classed as a data breach and as such must be immediately reported to the Academy Principal or Trust Data Protection Officer. The Trust has an obligation to report data breaches to the Information Commissioners Office (ICO) within 72 hours.
- Loss of data/equipment may result in disciplinary action.

17.0 REMOTE TEACHING AND LEARNING

Please refer to MLTs 'Remote Learning Guidance' document.

18.0 MOBILE DEVICES AND PORTABLE STORAGE

- Any Academy/Trust mobile device that may leave site and contain sensitive data must be managed by Office 365 Endpoint Manager and have policies enforced to ensure the protection of such data. This will include, patch management, anti-virus, access restrictions and device encryption.
- The use of portable storage (e.g. portable hard drives, memory sticks) is restricted across Trust and policies are in place to enforce this.

19.0 IMPLEMENTATION OF THE POLICY

- Access to systems is governed by role within the Academy/Trust. Procedures are in place to monitor any increase or decrease in access.
- Various protection solutions are in place across Academy/Trust networks, including anti-virus, anti-phishing, firewall, web and email filtering solutions. Logs across these systems are regularly checked by ICT Support. E-mail alerts are in place for critical systems.
- Use of telephony systems is also logged and regularly checked.
- ICT Support can remotely access and view any computer on Academies networks. This may be used randomly to implement this policy and to offer technical support.
- ICT Support regularly check asset registers and marked items.
- Staff are requested to report any breach of this policy to Academy Principals or the Trust CEO.

Any breach will be acted upon in line with Trust policies.

Maltby Learning Trust can and will prosecute illegal actions covered by the following acts:

- General Data Protection Regulation (2018)
- The Computer Misuse Act (1990)
- The Copyright, Designs and Patents Act (1988)
- Copyright (computer programs) regulations (1992)
- Public Interest Disclosure Act (1998)
- Obscene Publications Act (1959)
- Telecommunications Act (1984)
- Theft Act (1968)

APPENDIX 1

ICT ACCEPTABLE USE AGREEMENT FOR STAFF, GOVERNORS AND VISITORS.

This agreement is designed to ensure that all staff, governors and visitors are aware of their responsibilities when using any Trust ICT systems. All staff, Governors and visitors are expected to sign this agreement and adhere to its contents at all times.

- I will only use Trust ICT facilities and any related technologies for Trust approved business.
- I will comply with all ICT security measures and not disclose any passwords provided to me by the Trust or other related authorities. I understand that I am responsible for the security of my account.
- I understand that I must not allow students to use my computer login/password.
- I will not install or make changes to any hardware or software without prior permission from ICT Support.
- I understand that my use of the Internet and other related technologies is monitored and logged, and these logs can be made available on request to the Trust CEO.
- I will not attempt to bypass filtered Internet connections while working on Trust sites, using for example personal hotspots on mobile devices.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that for any Trust employee, the publication or the electronic transference of any material that could be regarded as derogatory, relating to the Academy, its operations or stakeholders, is a disciplinary offence.
- I will only download files from trusted sources.
- I will only use approved communication systems for any Trust related business.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I understand that all reasonable precautions must be taken to avoid malware infection of Trust systems. Although phishing protection software is in place, I will still be vigilante and report any suspicious emails to ICT Support.
- I will support and promote the Trust's e-Safety policy and help children and young people and adults to be safe and responsible in their use of ICT and related technologies.
- I will not give out my own personal details, such as a mobile phone number and personal e-mail address, to students.
- I will respect copyright and intellectual property rights.
- I understand that data protection is a significant public issue, and I am familiar with the General Data Protection Regulation (GDPR).
- I will ensure that any personal data is kept secure and used appropriately, whether on site or accessed remotely. I understand that personal data should only be accessed remotely when authorised by the Trust.
- I will ensure that images of students and/or staff are only taken, stored and used for professional purposes in line with the Trust policy.
- I will ensure that my on-line activity, both within Trust and externally, will not bring my professional role into disrepute.

The Trust has a means to log network activity and may use these logs as evidence of misuse of the facility, or breach of the above conditions of use.

APPENDIX 2

ICT ACCEPTABLE USE AGREEMENT FOR STUDENTS - SECONDARY

Students must read and follow the conditions set out in this agreement when using ICT. If you need help or are unsure about anything written below, please ask a member of staff or refer to the main policy which supports this agreement. Any breach of the conditions below may lead to withdrawal of your access to ICT and the network.

PASSWORDS & SECURITY

- I will only use my own ID and password to log onto a computer.
- I will not give out my password to anyone. If I suspect anyone knows my password, I will ask for it to be changed.
- I will log off properly after I have finished with the computer.
- I will not access any other user's files and folders without permission.

ONLINE

- I will only use the Academy's Internet for school related work and educational purposes. I will not browse or download anything illegal.
- I will not create or share any material that is derogatory, may cause upset to others, or bring the Academy name into disrepute. If I do come across any such material, I will report it immediately to a member of staff.
- I understand why the Academy/Trust filters Internet content and I will not attempt to bypass the Internet filtering system.
- I will not attempt to access any social networking sites or chatrooms in school except those systems which are operated by, or for, the Academy/Trust for educational purposes.
- I will not attempt to buy goods or services via the Internet.

COMMUNICATION

- I will only use the Academy's approved communication systems for schoolwork.
- I will not use abusive or threatening language in an e-mail or chat.
- If I am unsure about opening or downloading the contents of an e-mail, I will ask a member of staff.

IMAGES

- I will only take, store, and use images of students and/or staff for agreed Academy/Trust projects or purposes.
- I will not use or re-distribute images or video of others without their explicit permission.
- I will be mindful of any image I post online or send via social media, knowing that once sent they can be difficult if not impossible to retrieve.

SAFETY

- I will not perform any actions which may compromise the stability or security of ICT services in the Academy/Trust.
- I will not disclose my personal details or share the personal details or images of others.
- I understand that people I may talk to online may not be who they say they are. I will not meet with anyone whom I contact via the Internet without obtaining permission from a parent, carer, or teacher.
- I know that all use of the network in the Academy/Trust is monitored, and many websites keep permanent records of any content I create or share.
- I will abide by copyright laws and will not plagiarise material from the Internet.

RESPECT

- I will only communicate with others politely and sensibly.
- I will treat other people and ICT equipment with care and respect.
- I will not attempt to move, tamper with, or modify school PCs including disconnecting any cables.
- I will not take food or drink near to any computer.
- I will contact the ICT Support Team if I suspect that any equipment is faulty.
- I will not print anything in school other than schoolwork and I will print responsibly.

It is my responsibility to respect and follow all the above conditions which will help to keep me and others safe while using ICT.

APPENDIX 3

ICT ACCEPTABLE USE AGREEMENT FOR STUDENTS – KS2

Respect

- When using ICT, I respect myself, others, and the equipment I use.
- This means I:

    - always ask permission before using ICT.
    - ask if I need help.
    - am careful with the equipment I use.
    - will tell an adult if something in school doesn't work properly.

Online

- I will always ask permission before using the Internet.
- I know that when I go online I will:

    - never deliberately search for something rude or violent.
    - always tell an adult if I see anything that makes me or my friends uncomfortable.
    - not believe everything I read on the Internet.
    - never open or download a file unless I know it is safe. If I'm not sure, I should ask an adult first.
    - respect copyright when using content from the Internet.

Communication

- When I communicate online using e-mail or social media, I communicate safely by:

    - always thinking and checking that what I write or post is kind, polite and respectful.
    - being kind to my friends and classmates and thinking about how the things I do or say online might make them feel.
    - not sending mean or bullying messages or forwarding them to other people.
    - speaking to an adult if someone is unkind to me or if I know someone else is upset or scared.
    - never talking to anyone I don't know.
    - telling an adult if someone asks to meet up with me in real life.

Protect

- I protect myself and others by being aware that my full name, photo, birthday, address and phone number is personal information and is not to be shared online.
- This means I:

    - stop to think about what I post or share online.
    - protect my friends' information in the same way.
    - protect my passwords and don't share them with anyone except my parent.
    - never answer questions online that ask for my personal information.

At school we/I have:

- Discussed ways to be a safe, responsible, and ethical user of ICT at school, home and everywhere.
- Presented my ideas around the ways that I can be a smart, safe, responsible, and ethical user of ICT.

APPENDIX 4

ICT ACCEPTABLE USE AGREEMENT FOR STUDENTS – KS1, EYFS

Key stage 1

- I will ask a teacher or adult if I want to use the computers or tablets.
- I will only use activities that an adult has allowed me to use.
- I will take care of computers, tablets, and any other ICT equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something on screen that upsets me.
- I know that if I break the rules, I might not be allowed to use a computer or tablet.

APPENDIX 5

DOMAIN DEVICE LOGON MESSAGE

'By signing on to this device, you agree to follow Maltby Learning Trust's Safe Use of ICT Policy and end user agreements.'