The Maltby Learning Trust

MLT Communications (Safe Use of ICT) Policy

Date Last Reviewed:	October 2018
Reviewed by:	ICT Team Leader
Approved by:	MLT Board
Next Review Due:	October 2019

Maltby Learning Trust

Statement of intent

Maltby Learning Trust believes that IT plays an important part in both teaching and learning over a range of subjects.

The Trust is committed to ensuring that both staff and students have access to the necessary facilities and support to allow them to carry out their work.

This policy covers the rules and procedures for authorised and unauthorised use of the IT and communication facilities and is implemented in conjunction with the Trust`s E-Safety policy.

1. OVERVIEW

1.1 The IT facilities Across Maltby Learning Trust are defined as:

- Computer and software
- Monitor
- Keyboard
- Mouse
- Printer
- Scanner
- Camera
- Camcorder
- Other devices including furnishings and fittings used with them

1.2 The communication facilities across Maltby Learning Trust are defined as:

- Telephone
- Fax machine
- Television
- Video player
- DVD player
- Satellite receiver
- Mobile phone
- CCTV
- Radio
- Other devices including fittings used with them

1.3 Internet and e-mail can be defined as a communication facility used in conjunction with IT facilities; as such, these will coincide with the IT facilities.

1.4 This policy contains:

- The Trust's view on the use of e-mail and the internet at work.
- An explanation on what you can or cannot do.
- The consequences if you fail to follow the rules set out in this policy.
- General information relating to IT, including the General Data Protection Regulation.
- How the policy is implemented?
- The ICT Technical Support duties to the IT policy.

2. POLICY

2.1 The use of the IT facilities across the Trust is encouraged, as its appropriate use facilitates communication and can improve efficiency.

2.2 Used correctly, it is a tool that is of assistance to employees. Its inappropriate use, however, can cause many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.

2.3 Staff should always be an example of good practice to the students, serving as a positive role model in every aspect.

2.4 Abuse of the IT facilities could result in the facilities being removed. Staff should always be aware of IT use, and misuse of the facilities, as defined in this policy, must be reported to the Academy Principal.

2.5 Students misusing the IT facilities must be reported to the Academy Principal.

2.6 This policy applies to any computer/device connected to the Trust's network and computers.

2.7 Any breach of the rules in this policy may result in disciplinary action being taken and may lead to dismissal.

2.8 A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the Trust.

3. PROCEDURE

3.1 The Trust's e-mail system and internet connection are available for communication and use on matters directly concerned with Trust's business.

3.2 Employees using the Trust's e-mail system and internet connection should give particular attention to the following points in this policy.

- E-mail should not be used as a substitute for face-to-face communication, unless it is otherwise impossible.
- "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage work relationships.
- Hasty messages, sent without proper consideration, can cause unnecessary misunderstanding.
- If an e-mail is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.
- The Trust will be liable for any defamatory information circulated either within the Trust or to external contacts.
- The Trust's e-mail system and accounts must never be registered or subscribed to unsolicited e-mail (SPAM).
- Never disclose any of the Trust's e-mail addresses without confirming that they will not be subjected to SPAM and that they will not be sold on to marketing companies.
- All e-mails that are sent or received must be retained within the Trust for a period of six months.
- All e-mails being sent to external recipients must contain the Trust's standard confidentiality notice. This notice will be configured as a signature by the IT Support Team and must not be removed.
- Non-text e-mails (containing graphics or colour) and e-mail attachments may contain harmful materials and computer viruses, which can seriously affect the IT facilities. If unsure, seek assistance or approval from the IT Support Team.
- Offers or contracts sent via e-mail or the internet are as legally binding as those sent on paper. An exchange of e-mails can lead to a contract being formed between the sender, or the Trust and the recipient. Never commit the school to any obligations by e-mail or the internet without ensuring that you have the authority to do so. If you have any concerns, contact the CFO or MLT ICT Strategic Leader.

- Online purchases are only permitted via the Finance team, in order to comply with monitoring and accountability. Hard copies of the purchase must be retained for the future use by the purchaser and the business/finance manager. This is in addition to any purchasing arrangement outlined in the Trust's Financial policies.
- Failure to follow these procedures satisfactorily may result in disciplinary action, including summary dismissal.

4. AUTHORISED USE OF THE IT FACILITIES

4.1 The IT facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, curricular and enrichment activities, meetings, reviews, etc.
- Researching for any Trust related task
- Any trust encouraged tuition or educational use
- Trust business activities
- Access to your personal e-mail must never interfere with your work duties.

5. AUTHORISED USE OF THE COMMUNICATIONS FACILITIES

5.1 The communication facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, curricular and enrichment activities, meetings, reviews, etc.
- Researching for any Trust related task
- Any Trust encouraged tuition or educational use
- Trust business activities
- If unsure about your required use, please seek authorisation from the CEO.

6. UNAUTHORISED USE OF THE IT FACILITIES

6.1 It is not permitted under any circumstance to:

- Use the IT facilities for commercial or financial gain without the explicit written authorisation from the CEO.
- Physically damage the IT facilities.
- Re-locate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the IT Support Team or Academy Principal. Certain items are asset registered and security marked; their location is recorded by the IT Support Team for accountability. Once items are moved after authorisation, staff have a responsibility to notify the IT Support Team of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the IT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone. This is illegal under the Computer Misuse Act.

- Use the IT facilities at any time to access, download, send, receive, view or display any of the following:

    - Any material that is illegal
    - 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

- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- 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 IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the Trust's computers. This is illegal under the Computer Misuse Act.
- It is illegal to use or attempt to use the Trust's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not.
- Purchase any IT 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 or attempt to use the Trust's phone lines for internet or email access unless given authorisation by the CEO. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, you must not download or attempt to download any software.
- 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 Trust's networks or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the IT facilities for personal use without the authorisation of the CEO. This authorisation must be requested on each occasion of personal use.
- 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.
- To 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 IT facilities.
- Be wasteful of IT resources, particularly printer ink, toner and paper.
- Use the IT facilities when it will interfere with your responsibilities to supervise students.

6.2 Any unauthorised use of e-mail or the internet is likely to result in disciplinary action including summary dismissal.

6.3 If you are subjected to, or know about harassment or bullying, you are encouraged to report this immediately to your line manager or the CEO.

7. UNAUTHORISED USE OF THE COMMUNICATIONS FACILITIES

7.1 It is not permitted under any circumstance to:

- Use the communication facilities for commercial or financial gain without the explicit written authorisation from the CEO.
- Physically damage the communication facilities.
- Use the communication facilities for personal use without authorisation from the Academy Principal with the exception of the circumstance in 7.2.
- Re-locate, take off-site or otherwise interfere with the communication facilities without the authorisation of the CEO.
- Use the communication facilities at any time to access, receive, view or display any of the following:
    - Any material that is illegal
    - Any material 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
    - 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 material
    - Any adult or chat-line phone numbers

- Use or attempt to use the Trust's communication facilities to undertake any form of piracy, including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal.
- Use or attempt to use the Trust's communication facilities for internet or e-mail access unless given authorisation by the CEO. This includes using or attempting to use any other form of hardware capable of telecommunication regardless of ownership.
- Copy, record or distribute any material from or with the communication facilities that may be illegal. This can include television media, films, telephone conversations and music. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- Use or attempt to use the communication facilities to call overseas without the authorisation of the Academy Principal.
- Use the communication facilities when it will interfere with your responsibilities to supervise students.

7.2 Use of the Trust's telephone facilities for personal use is permitted for necessary calls lasting less than 10 minutes. Should you need to use the telephones for longer than this, then authorisation must be sought from the Academy Principal. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls. Any personal use of the telephones may be subject to a charge; this is at the Principal's discretion.

7.3 Certain items are asset registered and security marked, their location is recorded by the IT Support Team for accountability. Once items are moved following authorisation, staff have a responsibility to notify the financial assistant of their new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

7.4 If you are subjected to or know about harassment or cyber-bullying, you are encouraged to report this to your line manager or CEO.

8. IMPLEMENTATION OF THE POLICY

8.1 Staff are requested to report any breach of this policy to the CEO.

8.2 Regular monitoring and recording of e-mail messages will be carried out on a random basis. Hard copies of e-mail messages can be used as evidence in disciplinary proceedings.

8.3 Use of the telephone system is logged and monitored.

8.4 Use of the Trust's internet connection is recorded and monitored.

8.5 The MLT ICT Strategic Leader randomly checks asset registered and security marked items.

8.6 The IT Support Team checks computer logs on the Trust's network regularly.

8.7 Unsuccessful and successful log-on are logged on every computer connected to the Trust's network.

8.8 Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.

8.9 The IT Support Team can remotely view or interact with any of the computers on the Trust's network. This may be used randomly to implement the IT Policy and to assist in any difficulties.

8.10 The Trust's network has anti-virus/anti-malware software installed with a centralised administration package; any virus found is logged to this package.

8.11 The Trust's MIS database systems (SIMS) are computerised. Unless your line manager gives you express permission, you must not access the system. Failure to adhere to this requirement may result in disciplinary action.

8.12 All users of the Trust's MIS database system (SIMS) will be issued with a unique individual password, which must be changed at regular intervals. Do not, under any circumstances, disclose this password to any other person.

8.13 Attempting to access SIMS using another employee's user account/password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

8.14 User accounts are accessible by the IT Support Team with approval from the account holder, unless there is a requirement to access an account in the event of an investigation

following a breach of ICT Policy; in such an event, the CEO will provide the necessary authorisation to access the account.

8.15 Users are required to be familiar with the requirements of the General Data Protection Regulation, and to ensure that they operate in accordance with the requirements of the Regulation. The obligations under the Act are complex but employees must adhere to the following rules (further detailed information is included in the Trusts Data Protection Policy).

8.16 Do not disclose any material about a person, including a pupil, without their permission. Such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences.

8.17 Do not send any personal data outside the UK

9. GENERAL IT INFORMATION

9.1 Messages should be deleted after six months or stored in a suitable hard/soft copy file.

9.2 Information and data on the Trust's networks and computers should be kept in an organised manner and should be placed in a location of an appropriate security level. If unsure, please seek help and information from the IT Support Team.

9.3 Employees who feel that they have cause for complaint as a result of e-mail communications 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.

10.WORKING REMOTELY

10.1 Remote working refers to any work done outside the Trust, including accessing, storing, processing or discussing academy information. This could be at home, mobile working; traveling on public or private transport; staying in hotels; in public places such as libraries or coffee shops or even having telephone conversations in the street. All users of Maltby Learning Trust's ICT systems, equipment and information 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.

10.2 When working from home 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.

10.3 Make sure your location is sensibly secure to work in, for example it is not overlooked. Do not work on sensitive matters in a public place. If working from home, if possible, use a room where the door can be closed. Use the security options on your mobile phone, such as a pin number or a password.

10.4 Removable media containing academy information must be encrypted by the Trust's ICT Support team. Contact the ICT Support Team, if travelling or working overseas, to check whether security restrictions apply.

11.DATA PROTECTION GUIDANCE

11.1 All staff within the Trust should bear in mind that the loss or misuse of personal data is an offence under the General Data Protection Regulation.

11.2 Unattended computers must be turned off or locked and password protected.

11.3 Documents containing information which is classed as Protected, Restricted or Confidential must be disposed of via the confidential bins/bags which are available via the caretakers. (See Data Classification Table below for details) e.g. Visit/Trip lists, Learning Cycle Reports exported from SIMS, SEN/Medical data.

12.C:\ DRIVE – YOUR COMPUTER'S INTERNAL HARD DRIVE (INCLUDING THE DESKTOP)

12.1 The C:\ drive is not backed up. If your laptop or computer is lost, stolen or damaged you will not be able to retrieve data from the C:\ drive. Furthermore, data stored on C:\ can easily be accessed if your device is stolen.

12.2 Because of this you must not store ANY data on your C:\ drive – this includes emails.

12.3 If you currently have any student/staff information on your computers C:\ Drive in school or at home, this must be either deleted or immediately moved to your Home drive on the network.

12.4 Photographs of students must only be stored in a secure area of the network that is not accessible by students. If a student needs access to a photograph for a particular project these should be distributed by staff to individual students and not given to a whole group.

13.MEMORY STICKS

13.1 A memory stick, USB drive, flash drive is a portable storage device.

13.2 If you need to take Protected, Restricted or confidential data outside of the Trust this must be done via an encrypted laptop/memory stick. See the ICT Support Team for more details.

14.WORKING OUTSIDE THE TRUST

14.1 When you remove equipment, files and data from the Trust you are responsible for ensuring its safe transit and storage.

14.2 Information off-site / at home must only be used for work related purposes

14.3 When no longer required, paper/files/disks etc. must be returned to the Trust and disposed of via the confidential waste destruction system.

14.4 Any member of staff allowing access to an unauthorised person, deliberately or inadvertently, may be subject to disciplinary proceedings.

14.5 You must only remove files and equipment from the workplace where there is a business need to do so and they should be returned as soon as possible.

14.6 Information which is classed as PROTECTED must not be sent to or from home via email as the information is not secure once it leaves the Academy.

14.7 Files and equipment should not normally be left in an unattended vehicle. If it is absolutely necessary to leave something in a vehicle, lock it in the boot. However, if files or equipment contain information which is classed as PROTECTED they must not be left in a vehicle except in an emergency situation.

14.8 Information which is classed as PROTECTED or above (See Data Classification Table below for details) must not be shared with family members. Only authorised members of staff are allowed access to information being used at home in any form, on any media. No family members are allowed access to the equipment or information.

14.9 Information which is classed as PROTECTED or above (See Data Classification Table below for details) must be neatly filed and stored away when not in use. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase).

14.10 When Files or Equipment are stored at home they should not be openly accessible to other members of the household or visible from outside the premises.

14.11 Loss of equipment must be reported to the ICT Support Team. All thefts/losses of equipment will be reported to the police. Loss of data/equipment may result in disciplinary action.

15.DATA CLASSIFICATION DEFINITIONS

Data Type	**Examples**	**Impact if the data is lost or stolen and misused**
UNRESTRICTED	• Information published on the Academy Web Site or is otherwise publicly available • Information that would be disclosed in response to a Freedom of Information Request • Disclosure will not adversely affect a client or member of staff	• None / negligible

PROTECTED	• Personal data relating to any • student or member of staff such as a name, address or any personal identifier, • Any other data considered to • be covered by the Data • Protection Act. i.e. SEN, medical, learning cycle data, score cards, phone numbers • Any data which may result in financial loss. i.e. FMS data • Any data which is considered to be	• Inconvenience to clients • Damage to the Academies standing or reputation
RESTRICTED	• A complete record containing • many personal details. i.e. Names, addresses, phone numbers, medical records • Volumes of "PROTECTED" data about a large number (10+) of students or staff i.e. Personnel records, • Admission forms, names and addresses, SEN, medical, phone numbers, salaries	• Substantial inconvenience or distress • Significant impact to a client • Substantial damage to the Academies standing or reputation • Prejudice the investigation of or • Facilitate the commission of crime • Could have wider implications for the Academies finances or reputation

16.CONNECTING TO THE ACADEMY FROM HOME

16.1 When connecting from home you will have access to your My Documents and all shared drives/resources. SIMS will also be accessible. Any data held within SIMS must not be transferred outside of the Academy. Any data exported, i.e. mark sheets/LC data must be saved to your Documents on the network and not emailed home or saved on un-encrypted USB memory pens.

16.2 You must log in using your own username and password when connecting from home and you must never leave an unattended computer logged in.

16.3 Any member of staff allowing access to an unauthorised person, deliberately or inadvertently, may be subject to disciplinary proceedings.

16.4 Information classed as Protected, Restricted and Confidential should not be emailed home and saved on your home computer, see table above.

16.5 Information classed as Protected, Restricted and Confidential data should never be saved to an un-encrypted USB/memory stick, see table above.

17. ACCEPTABLE USE AGREEMENT

STAFF, GOVERNOR AND VISITOR ACCEPTABLE USE AGREEMENT/CODE OF CONDUCT

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life within the Trust. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

I will only use the Academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed "reasonable" by the CEO or Trust Board.

I will comply with the ICT system security and not disclose any passwords provided to me by the Trust or other related authorities.

I will ensure that all electronic communications with students and staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal email address, to students.

I will only use the approved, secure email system(s) for any Academy business. The only personal usage tolerated is in the following areas:

- It is in the user's own time i.e. outside normal working hours
- It does not interfere with work performance or divert employees from their duties
- It is not used for furthering outside business interests or for personal monetary gain
- The use of the Internet conforms to all other requirements in this policy
- Usage does not adversely affect the performance of the e-mail system or Academy network.

A minimal level of mundane personal use is tolerated. This use must be outside your working time. Be aware that emails may be monitored and that personally sensitive information should not be sent. Messages should not contain anything that others may find offensive or distasteful. Examples of material that is not permitted are those with a sexual content, jokes or chain letters etc. Personal encryption of messages is prohibited.

If you receive messages which breach this policy, then you should do the following:

- If you know the sender, reply advising them that Trust's Policy prohibits that type of message and ask them not send any more similar messages.
- If the message is from another Academy employee, then contact your Line Manager for further advice.
- If you are offended or upset by the message you should refer to the Bullying and Harassment Policy, discuss it with your Line Manager or the CEO.

- If the message is from outside the Trust and you do not know the sender, then advise the ICT Support Team who can arrange to have messages from specified senders blocked.

I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in the Academy, taken off the Academy premises or accessed remotely. Personal data can only be taken out of Academy or accessed remotely when authorised by the CEO or Trust Board.

I will not install any hardware or software without permission of the ICT Support Team.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Images of students and/ or staff will only be taken, stored and used for professional purposes in line with the Trust's policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Academy network without the permission of the parent/carer, member of staff or CEO.

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or CEO.

I will respect copyright and intellectual property rights.

I will ensure that my online activity, both in Academy and outside Academy, will not bring my professional role into disrepute by posting defamatory comments about the Trust or its Academies on social media sites, e.g. Twitter, Facebook, etc.

I will support and promote the Trust's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

Internet access is restricted through the use of web filtering software which prohibits the majority of inappropriate or offensive material. Under no circumstances should this be bypassed in the Academy with the use of any other device, (Example, USB broadband dongles, Mobile phone hotspot)

I understand the publication or the electronic transference of any material that could be regarded as derogatory, relating to the Academy, its operations, its staff or its students is a disciplinary offence, which could lead to dismissal.

The accessing and appropriate use of Trust data is something that the Trust takes very seriously.

Staff are aware of their responsibility when accessing Academy data. Level of access is determined by the Network Manager.

Any data taken off the Academy premises must be encrypted.

I understand that Data Protection is a significant public issue and for the protection of all involved in the Academy the additional Student Information Protocol needs to be adhered to by all staff.

I understand that all reasonable precautions must be taken to avoid virus infection of the Trust's computer system. Deliberate downloading of viruses is a disciplinary offence. Any virus detected must be reported to the IT Support Team immediately.

I understand that professional and personal etiquette are a central part of our way of working. Mutual respect between colleagues is as vital in electronic communications as it is in face to face conversations.

I understand that I must not allow students to use my computer login/password.

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

Agreement

I agree to observe all the conditions in the Trust's Policy for users being provided with Internet Access. I understand that violation of these rules will result in disciplinary action which could involve sanctions up to and including dismissal.

Signature: _____ Date: _____

Full Name: _____(Print)

Job Title: _____