Electronic Information and Communications Systems

Name of Policy	ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY
Policy Level	Trust
Date of issue	October 2019
Author:	Trust Board
Date of Next Review:	October 2020
Signature	
Date of Signature:	16th December 2019

Table of Contents

Introduction

The Trust's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the Trust who are required to familiarise themselves and comply with its contents. The Trust reserves the right to amend its content at any time.

This policy outlines the standards that the Trust requires all users of these systems to observe, the circumstances in which the Trust will monitor use of these systems and the action the Trust will take in respect of any breaches of these standards.

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018 together with the General Data Protection Regulations 2018 (GDPR) and Employment Practices Data Protection Code issued by the Information Commissioner.

Staff are referred to the Trust's Data Protection Policy for further information. The Trust is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the Trust's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Trust's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The Trust has the right to monitor all aspects of its systems, including data which is stored under the Trust's computer systems in compliance with the Data Protection Act 2018.

This policy mainly deals with the use (or misuse) of computer equipment (hardware, software and data), computer network e-mail, internet connection, online tools, telephones, iPads (and other mobile device tablets), Blackberries, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like by all staff.

Schedule of Responsibilities

The CEO of Learning Today leading Tomorrow Trust (LT2) takes overall responsibility for the implementation of policies and procedures and to provide reports as appropriate to Trustees in relation to this policy.

Headteachers of LT2 schools and their Senior Leadership Teams will take active steps to promote good practice under this policy and review and monitor the management and implementation of this policy and practice in their Academy. They will identify training needs, ensuring competence in those staff who are responsible for and involved in the operation of this policy and associated guidance.

Teachers and other supervisory roles will, where required, conduct formal meetings, undertake relevant training in relation to this policy and ensure effective and competent operation of this policy.

All employees are required to cooperate fully and positively with the requirements of this Policy and to undertake any training recommended by their line manager.

The Trust's HR Advisers, are responsible for providing advice and guidance under this policy and reviewing and updating the policy as required; ensuring continuing compliance in line with any developments in employment legislation, good employment practice and other LT2 policies. The Trust's HR Providers may be requested to provide data for regular Trust Board HR reports where appropriate, providing confidential reports as required by the CEO and LT2 Trust Board on individual cases.

The following persons will generally be responsible for managing employees under this policy:

- The Academy Headteacher (for Academy based teaching and educational or non-educational support staff); and,
- The Chief Executive Officer (for Academy Headteachers and centrally appointed teaching and support staff) (the "Line Manager").

Acceptable Use of ICT Equipment

The Trust is committed to safeguarding its computing system to ensure it can be used in the most effective manner to support the teaching and learning processes and enable The Trust's business tasks to be undertaken. Ensuring the safety and integrity of the Trust's ICT system is the responsibility of all staff.

The Trust encourages staff to fully use the computing infrastructure and to make use of Mobile Computer Devices equipment offsite to support them in their work. The Trust encourages this use in a responsible and professional manner. Mobile devices include for example laptops, tablets, notebooks, smartphones and other portable/mobile devices.

As a user of the Trust's Computer systems you have a right to use it responsibly. These user responsibilities are outlined below. Misusing the Trust's computing systems may breach this and other Trust policies.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Staff are advised of this policy during their induction and of the Trust's requirement for them to adhere to the conditions therein.

For the purposes of this policy the term "computing services" refers to any computing resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own device to the Trust's network and the services available are particularly reminded that such use requires compliance to this policy

Purposes

- To protect the Trust's networks and equipment
- To protect the Trusts data
- To protect the Trust and its employees from activities that might expose them to legal action from other parties

Guidelines

Equipment Security

All members of staff should adhere to the following guidelines when using computing equipment provided by the Trust. The employee (must):

- Is responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy;
- Treat equipment safely, in the same manner as a reasonable person would;
- Keep liquids away from ICT equipment;
- Do not place heavy objects on ICT equipment;
- Do not drop ICT equipment or objects onto it;
- Any portable computer must be securely locked away when not in use;
- Portable computer security is your responsibility at all times;
- Do not leave the portable computer unattended in a public place or within the Trust;
- Do not leave the portable computer inside your car;
- Take extra reasonable care to prevent the loss of any removable storage device which contain confidential Trust data;
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment.

Password Security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the Trust.

Issuance and continued use of your User Account is conditional on your compliance with this policy.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Staff are required to select a password that cannot be easily broken and which contains at least 12 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with members of the ICT staff or ICT partner as appropriate and necessary. Staff must assume personal responsibility for usernames and passwords for all accounts and sites connected with their employment at the Trust

Any member of staff who discloses his or her password to another employee in the absence of express authorisation are in breach of this policy and will be liable to disciplinary action under the Trust's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password are in breach of this policy will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords are set by policy to expire every 30 days so users are forced to change their passwords. Passwords should be changed immediately if the user believes or suspects that their account has been compromised.

If given access to the Trust e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team and/or members of the ICT staff or ICT partner may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of members of the ICT staff or ICT partner.

On the termination of employment for any reason, staff are required to provide details of their passwords and provide a full handover detailing the drives, folders and files where their work can be located and accessed. The Trust reserves the right to require employees to hand over all Trust data held in computer useable format.

Members of staff who have been issued with a laptop, iPad (and other mobile device tablets), PDA or Blackberry must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

General Conditions

In general, use of Trust "computing services" should be for your/the user's study, research, teaching or the administrative purposes of the Trust. Some use of the facilities and services for personal use is accepted, so long as such activity does not contravene the conditions of this policy.

- Your use of the Trust's computing services must at all times comply with the law.

- Your use of the Trust's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer/device that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the user's permission.
- You must not use Trust computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use Trust computing services for the creation, modification, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Headteacher).
- You must not use the Trust's computing services to conduct any form of commercial activity without express permission.
- You must not use the Trust's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a license, and which is not first authorised by the ICT technicians for installation
- You must not use any P2P/torrent client as these enable illegal sharing of copyrighted material
- You must not use any IRC or messenger software including, but not limited to WhatsApp, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorised to do so for work related purposes You must not use any Messenger Software, including but not limited to WhatsApp, Hangouts, Internet Relay Chat (IRC), unless authorised to do so from the Principal for work related purposes.
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the Trust facilities, unless specifically related to Trust activities
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Executive Principal/Governing Board
- You must not play computer games of any nature whether preinstalled with the operating system or available online unless it has been agreed by your line manager as having educational value for children or it is outside of your working hours

Systems Use and Data Security

The Trust holds a variety of sensitive data including personal information about students/pupils and staff. If you have been given access to this information, you are reminded of your responsibilities under the Data Protection Act 2018 and General Data Protection Regulations 2018 (GDPR).

Members of staff should not delete, destroy or modify any of the Trust's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the Trust, its staff, students, or any other party.

You should only take a hard copy of data outside the Trust's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, any removable encrypted storage device, and cloud storage or into secure emails, also personal cloud storage solutions (example: MS OneDrive, Google drive, iCloud) for the transfer of Trust information is expressly forbidden.

If you do need to take data outside the Trust, this should only be with the authorisation of the Trust's GDPR Champion. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop or terminal services) which allow you to work on data in-situ rather than taking it outside the Trust, and these should always be used in preference to taking data off-site.

Our ICT partner and ICT staff offer a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from members of the ICT staff who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems. If in doubt, the employee should seek advice from members of the ICT staff or ICT partner or a member of the Senior Leadership Team.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming;
- Instant messaging;
- Chat rooms;
- Social networking sites; and,
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to our systems without the prior approval of members of the ICT staff or Senior Leadership team. This includes, but is not limited to, any PDA or telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player, infra-red or Bluetooth connection device or any other device.

The Trust monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). Members of the ICT staff or ICT partner should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The Trust also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the Trust's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the Trust's Systems and guidance under "E-mail etiquette and content" below.

Anti-Virus and Firewall Security

All Trust devices are installed with current versions of virus protection and firewall software by ICT staff. Users cannot alter the configuration of this software and no attempt should be made to do so by any means. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the ICT staff or ICT.

Remote Access

Remote access to the Trust network is possible where this has been granted by the ICT staff.

Remote connections are considered direct connections to the Trust network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car;
- Laptops must be carried as hand luggage when travelling;
- Information should be protected against loss or compromise when working remotely (for example at home or in public places) through use of a VPN; and,
- When working in a public place, staff must use a privacy screen.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available to the Network

Manager and ICT staff and partner and kept for no longer than necessary and in line with current data retention schedule.

Such records and information are sometimes required - under law - by external agencies and authorities. The Trust will comply with such requests when formally submitted.

Use of Personal Devices

Where staff use their own personal equipment such as mobile telephones, laptops, notebooks, tablets etc, if they are on Trust premises, or being used to access Trust data from anywhere, this must be with the permission of the Trust and the devices must be secure with confidential passwords.

Staff who use personal devices to access work emails / servers will need to sign to the personal devices log to confirm that their device / phone is password protected and encrypted.

Use of Telephones, Email and Internet by Staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the internet on a device. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This Policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the Internet.

The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure.

This Policy has been designed to safeguard the legal rights of members of staff under the terms of the Data Protection Act, GDPR and the Human Rights Act.

Use of Telephones

There will be occasions when employees need to make short, personal telephone calls on Trust telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of Trust telephones for private purposes, which are unreasonably excessive or for Trust purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the Trust has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the Trust reserves the right to record calls.

Use of Email

E-mail etiquette and content

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline. The Trust's e-mail facility is intended to promote effective communication within the business on matters relating to the Trust's business activities and access to the Trust's e-mail faility is provided for work purposes only.

Staff are permitted to make reasonable personal use of the Trust's e-mail facility provided such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the Trust's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The Trust encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the Trust's best practice.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e- mails should be retained on the appropriate file.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the Trust. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Trust in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The Trust standard disclaimer should always be used on every e-mail.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Group immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform your Line manager/Head of Department or the Headteacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the Trust's formal grievance procedure. (Further information is contained in the Trust's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

Where the Trust has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The Trust also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

General Guidance

Employees should:

- Not send any email, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;

- Not send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Be careful that before opening any attachment to an email they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law.
- Not send or forward private e-mails at work which they would not want a third party to read;
- Not send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the Trust;
- Not contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Not sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals;
- Not agree to terms, enter into contractual commitments or make representations by email unless the appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written in ink at the end of a letter;
- Not download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Not send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Not send messages from another worker's computer or under an assumed name unless specifically authorised;
- Not send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature;

The Trust recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. Your Data Protection Champion (see Data Protection Policy) and the Headteacher should be informed as soon as reasonably practicable.

Use of the web and the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the Trust, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the Trust's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the Trust (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the Trust's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use Trust systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e- mail such content to others unless certain that the owner of such works allows this.

The School's website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The Trust may publish relevant information on its own internal systems for the use of all staff. All such information is regarded as confidential to the Trust and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the Trust. Any exceptions to this must be authorised by a member of the ICT staff or ICT partner who will liaise with the Senior Leadership Team as appropriate and necessary.

Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The Trust reserves the right to audit the use of the Internet from particular Personal Computers/devices or accounts where it suspects misuse of the facility.

Personal use of the Trust's systems

The Trust permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

The following conditions must be met for personal usage to continue:

(a) Use must be minimal and take place substantially out of normal working hours (that is, during the member of staff's usual break time or shortly, before or after normal working hours);

(b) Personal e-mails must be labelled "personal" in the subject header;

(c) Use must not interfere with business or office commitments;

(d) Use must not commit the Trust to any marginal costs;

(e) Use must comply at all times with the rules and guidelines set out in this policy;

(f) Use must also comply with the Trust's compliment of operational policies and procedures including but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Excessive or inappropriate personal use of the Trust's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

The Trust reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

Inappropriate use of equipment and systems

Reasonable personal use is permissible provided it is in full compliance with the Trust's rules, policies and procedures (including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure).

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the Trust's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing

nature), racist or other inappropriate or unlawful materials;

(b) transmitting a false and/or defamatory statement about any person or organisation;

(c) sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;

(d) transmitting confidential information about the Trust and any of its staff, students or associated third parties;

(e) transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Trust;

(f) downloading or disseminating material in breach of copyright;

(g) copying, downloading, storing or running any software without the express prior authorisation of members of the ICT staff or ICT partner.

(h) engaging in on line chat rooms, instant messaging, social networking sites and on line gambling;

(i) forwarding electronic chain letters and other materials;

(j) accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the Trust may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

Monitoring the Use of Telephone, E-mail and the Internet

It is not the Trust's policy, as a matter of routine, to monitor an employee's use of e-mail service or of the Internet via the Trust's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Headteacher, CEO or Trust Board may grant permission for the auditing of an employee's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Headteacher.

These individuals are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Executive Principal/Governing Body or their delegated representative to enable Human Resources to advise the appropriate line manager/head of faculty the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

Safe Use of Management Information Systems

Principles

This applies wherever access to the Trust Management Information Systems (MIS) are provided. This applies to all online resources provided by the Trust, for example Capita SIMS. This policy applies whenever information is accessed through the Trust MIS, whether the computer equipment used is owned by the Trust or not. The policy applies to all those who make use of the Trust's MIS resources.

Purposes

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of the Trust's data, the Authorised MIS User and the individuals to which the MIS data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials;
- The wrongful disclosure of private, sensitive, and confidential information;
- Exposure of the Trust to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This Policy aims to ensure all relevant aspects of the Data Protection Act (2018) and GDPR (2018) are adhered to.

This Policy aims to promote best use of the MIS system to further the communication and freedom of information between the Trust and Parents/Carers.

Guidelines

The Trust's MIS system is provided for use only by persons who are legally responsible for student(s)/pupils currently attending the Trust. Access is granted only on condition that the individual formally agrees to the terms of this Policy.

The authorising member of Trust staff must confirm that there is a legitimate entitlement to access information for students/pupils the names of whom must be stated on the Online Usage Policy Declaration.

A copy of the form will be held by the Trust for audit purposes.

Personal Use

Information made available through the MIS system is confidential and protected by law under the Data Protection Act 2018, and GDPR. To that aim:

- Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the student/pupil to which the information relates or to other adults with parental/carer responsibility
- Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to the Trust in writing to the Network Manager and Headteacher.

The Trust reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

- The validity of parental/carer responsibility is questioned;
- Court ruling preventing access to child or family members is issued;
- Users found to be in breach of this policy

If any child protection concerns are raised or disputes occur the Trust will revoke access for all parties concerned pending investigation.

Upon Leaving the Trust

Upon leaving the Trust, members of staff must return all equipment and information, including equipment and data on or before the agreed leaving date (eg last day of employment) to their Line Manager or other School representative.

This includes, but is not limited to:

- All information, including data, used or stored as part of the role, both physical and electronic;

- All information, including files, documents and emails, including any data stored within individual accounts;
- Access control and ID cards;
- After leaving members of staff may not attempt to access or use any Academy information, including any data.

Breaches of this policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

In the event a Portable Computer/ Mobile Device is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the Trust.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

- Taking food and/or drink into rooms with computing facilities where they are forbidden.
- Sending nuisance (non-offensive) email.
- Behaving in a disruptive manner.

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12-month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libelling another person.
- Misuse of software or software license infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Examples of this level of breach would include but are not limited to:

- Repeated moderate breaches.
- Theft, vandalism or willful damage of/to Computing facilities, services and resources.
- Forging email i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.
- Any action, whilst using Trust computing services and facilities deemed likely to bring the Trust into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy Computing systems security.
- Attempting to modify, damage or destroy another authorised users data.

- Hacking into the Trust's network infrastructure to disrupt network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by Leadership under the direction of the Headteacher. That investigative report will be passed to the staff member's Line Manager, to be considered within the Trust's disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.