Aim High, Achieve Together, Celebrate Success

LT2 Information Security Policy

Name of Policy	INFORMATION SECURITY	
Policy Level (Trust/School)	Trust	
Document Control		
Date	**Revision Amendment Details**	**By whom**
March 2022	Review and internal consultation	Trust Strategic IT Manager and GDPR Lead
March 2022	Adopted by Trust Board	Trustees
March 2023	Proposed date for review subject to statutory update as required	Executive Team

Table of Contents

LT2 Vision, Mission and Values

Vision

Vision is to build a group of outstanding schools across phases, including specialist provision, to become (a mid-size) Trust that provides vibrant and inclusive learning environments in which every member of the learning community is passionate about learning. The Trust is led by a CEO who works closely with Headteachers who lead the two schools supported by a central team to support finance, HR, estates and governance.

Mission

LT2 Trust and schools will have a relentless focus on high achievement, supported by robust organisational structures and governance. We aim to give children and young people in our care the knowledge, skills and experiences to expand their minds and world view to enable them to develop a naturally inquisitive approach to learning and life, fit for an ever-changing world.

Ultimately, we will educate and support all children attending LT2 schools to grow into capable and contributing citizens who have developed the personal attributes and characteristics that will enable them to become considerate, self-reliant and confident young people who are ready for the next stage of their lives.

Values

The Trust Values underpin the mission and provide the basis on which LT2 schools can articulate the key behavioural characteristics that promote a positive philosophy. Our six values are unseen drivers of our behaviour as experienced by others and are designed to create a shared organisational culture:

Kindness – The quality of friendliness, generosity, and consideration

Collaboration – The belief that working and learning with others will lead to greater success

Curiosity – A strong desire to know and to learn

Resilience – The ability to recover quickly and learn from the difficulties we face

Respect – To appreciate the importance of understanding and admiration for others and self, honesty

Endeavour – The belief that hard work is needed to achieve something of which we can be proud

Definitions

- Where the word 'Trust' is used in this document it refers to The Learning Today Leading Tomorrow Trust.
- Where the words ‘Trust Board’ are used it refers to the board of Trustees who set the vision for the Trust and hold the executive leadership team to account for delivering the Trust’s strategic plan.

1. Organisation and Responsibilities

1.1 Introduction

The Objective of this Policy is to inform staff, governors and trustees and protect LT2 from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all staff, governors, and trustees of LT2 complying with this policy.

Staff responsibilities are outlined throughout this policy. Misusing the Trust's computing systems may breach this and other Trust policies. Ignorance of this policy and the responsibilities it places on employees, is not an excuse in any situation where it is assessed that an employee has 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.

1.2 Principles

LT2 has adopted the following six principles to underpin this Information Security Policy. All Personal data shall be:

- Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- Used for specified, explicit and legitimate purposes ('purpose limitation')
- Used in a way that is adequate, relevant and limited to what is necessary ('data minimisation')
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy')
- Kept no longer than is necessary ('storage limitation')
- Processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality')

1.3 Legislation

The Trust holds a variety of sensitive data including personal information about students/pupils and staff. If an employee has been given access to this information, they are reminded of their responsibilities under the Data Protection Act 2018 and UK General Data Protection Regulations .

1.4 Guidance under this Policy

The Trust Strategic IT Manager is responsible for providing advice and guidance under this policy and reviewing and updating the policy as required.

1.3 Board of Trustees

The Board of Trustees, as a corporate body, has the responsibility to set the strategic direction and objectives of all matters across the Trust.

The Board of Trustees is responsible for ensuring that high standards of corporate governance are maintained

The Chair of the Trust is responsible for managing the CEO, Trustees and Governors under this policy.

1.4 The Chief Executive Officer (CEO)

The CEO of Learning Today Leading Tomorrow Trust (LT2):

- Takes overall responsibility for the implementation of policies and procedures
- Must provide reports as appropriate to Trustees in relation to this policy
- Ensure that sufficient resources are allocated and authorised within the organisations budget to meet statutory procedures and standards across the Trust
- Is responsible for managing the Headteachers and centrally appointed staff under this policy

1.5 Headteachers

Headteachers of LT2 schools are responsible for:

- The implementation of and compliance with this policy within their school ensuring competence in those staff who are responsible for and involved in the operation of this policy and associated guidance
- Identifying training needs
- Communicating this policy to all relevant people within the school
- Managing school-based teaching and associate staff under this policy

1.6 Senior and Middle Leaders (and other Supervisory Roles)

Although the Headteacher is responsible overall for the implementation of this policy in their school, managers have some specific responsibilities:

- Applying this policy within their own department and area of work
- Resolving any issues members of staff refer to them, informing the Headteacher of any issues to which they cannot achieve a satisfactory solution with the resources available to them
- Where required, conduct formal meetings, undertake relevant training in relation to this policy and ensure effective and competent operation of this policy

1.7 Other Employee Duties

All employees have a responsibility to:

- Comply with this policy and to co-operate with the schools' leadership and management on all matters relating to it. Everyone has a role to play in ensuring security of information.
- Undertake any training recommended by their line manager

1.8 Related Policies and Procedures

- LT2 Data Protection Policy
- LT2 Monitoring Policy
- Individual school technical security guidance and procedures

1.9 Review

This policy will be reviewed annually. These procedures have been agreed by the board of trustees, who will approve them whenever reviewed.

2. 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 (guidance on remote working can be found in section 5).

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.

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.

The trust/schools' technical systems will be managed to ensure that the school meets recommended technical requirements.

2.1 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
- Portable computer security is the responsibility of the staff member to whom it is assigned at all times. Any portable computer must be securely locked away when not in use and not left unattended in public places
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment
- Staff without authorisation should only be allowed to use terminals under supervision.

2.2 General Conditions

In general, use of Trust "computing services" should be for an employee'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. Use of the trust's computing services must:

- At all times comply with the law
- Not interfere with any others' use of these facilities and services

Employees must not use the trust's computing services to:

- Access a computer/device that they have not been authorised to use
- Access any program or data which has not been specifically authorised for use
- Use or copy any data or program belonging to other users without their express and specific permission
- Alter computer material belonging to another user without the user's permission
- Harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person
- 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)
- Conduct any form of commercial activity without express permission
- Disseminate mass (unsolicited) mailings
- Install, use or distribute software for which you do not have a license, and which is not first authorised by the Trust Strategic IT Manager (or insert RFPS approving body) for installation
- Use any P2P/torrent client as these enable illegal sharing of copyrighted material
- Use any 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
- Access, download, store, transmit or run any material that presents or could present a risk of harm to a child
- Access audio or video streaming, chat rooms, online gambling, webmail (yahoo and Hotmail) and social networking sites unless expressly authorised to do so for work related purposes
- Post or subscribe to newsgroups, on-line discussion boards or email list groups from the Trust facilities, unless specifically related to Trust activities
- 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 Headteacher/CEO
- 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
- Tamper with any Desktop PCs and cabling for telephones without first consulting the Trust Strategic IT Manager

2.3 Anti-virus and Firewall Security

The purpose of this section is to establish requirements, which must be met by all devices within the trust computing infrastructure, to protect the confidentiality, integrity and availability of software and information assets from the effects of malware.

- All Trust devices are installed with current versions of virus protection and firewall software by ICT staff. 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
- Unless undertaken by or following instruction from IT support staff, staff must not disable anti-malware software running on, or prevent updates being applied to devices
- The intentional introduction of viruses to LT2 MAT's computing infrastructure will be regarded as a serious disciplinary matter
- Only software that has been authorised by the trust can be installed upon trust systems. Any employee wishing to download, install or run software from an external sources for work purposes must request permission from the Trust Strategic IT Manager/Headteacher. This includes instant messaging programmes and games. Where consent is given all files and data should always be virus checked before being downloaded.
- Each member of staff is responsible for immediately reporting any abnormal behaviour of computing systems to the Headteacher or the person with delegated responsibility for the IT system in the school
- Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party

2.4 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.

2.5 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. Trust Strategic IT Manager and School Operations Manager will keep an up to date records of users and their usernames. Issuance and continued use of a User Account is conditional on compliance with this policy.

All staff will be required to use two-factor authentication for Office 365 and other specific applications (when required).

Initial default passwords issued to any user should be changed immediately following notification of account set up. Any passwords set by a user should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters. They must not include proper names or any other personal information about the user that might be known by others.

Passwords should be changed at least every 90 days.

Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the school/trust

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.

Individual user IDs/passwords must be kept confidential and must not be shared or made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with IT staff as appropriate and necessary. They must not be written down and left with any equipment or accessible by anyone else. All employees are responsible for all transactions undertaken on their network logins and any connected with their employment at the trust.

Any member of staff who discloses their 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.

2.6 Email

When using their internal emails, employees should:

- Not send any email, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally
- Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others
- 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 emails 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
- Transmitting confidential information about the Trust and any of its staff, students or associated third parties
- Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Trust
- 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

Email 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 email facility 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 email first 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, AntiHarassment 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 their 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.

2.7 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. For example, employees must not access pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or other unlawful materials.

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 trust/school's websites are 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.

2.8 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.

2.9 Personal Use of Trust 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 section) 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.

2.10 Upon leaving the Trust

Upon leaving the trust, employees are required to return all equipment and information, including ID badges, access control and data (electronic and physical), on or before the agreed leaving date. They will also be 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. After leaving members of staff may not attempt to access or use any trust systems or data.

3. Creating, storing and managing information

LT2 has adopted both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.

The purpose of this section is to establish LT2 requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

3.1 Paper Information

Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other staff members at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.

- Confidential documents must not be left on display or unsupervised
- Store confidential information in locked cabinets, returning them to these cabinets when not required
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids
- Do not leave paper by printers or photocopiers where other people may take it or read it accidentally
- Spoiled photocopies and prints may still be confidential. Do not put them straight into the waste paper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies
- Dispose of confidential paper by shredding or via the confidential waste bins provided. Do not dispose of confidential waste in a waste paper bin or anywhere else
- Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records

3.2 Electronic Information

- All confidential information must be stored on LT2 approved electronic devices or systems with access controlled/restricted, e.g. the trust/school networks and other approved systems

- Confidential information must not be stored on local unencrypted hard drives. If confidential information has to be transferred to other portable media, such as USB stick or memory cards, it must be encrypted with appropriate security software approved by the trust/school
- PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g. through windows or while waiting in public areas. If this is not possible, a privacy screen should be used.
- Notebook PCs, handhelds or any other portable ICT device must not be left unattended in any public area (see Mobile Computing below)
- Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended. Employees are responsible for the security of their terminals. If an employee fails to lock their computer when left unattended they may be held responsible for another user's activities. SLT and IT Staff may do spot checks from time to time to ensure compliance.
- The use of personal cloud storage solutions for the transfer of trust information is prohibited
- Only those with authorisation must access the information stored on the MIS. The authoriser must confirm that there Is a legitimate entitlement to access information. 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

If an employee finds or access confidential information that they believe should be restricted, they should notify the Headteacher, Trust Strategic IT Manager or relevant Data Protection Champion immediately as this may constitute a Data Breach.

4. Receiving, sending and sharing information

An employee should have authorisation to take data outside of the trust and as part of this, they 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.

The following section outlines steps employees should consider when sharing data externally.

Transmitting confidential information about the Trust and any of its staff, students or associated third parties without authorisation is considered a breach of this policy.

4.1 Post

- Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays and 'pigeon holes'
- Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made

- If outgoing post contains confidential information to an individual, the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'. A return address must be shown on the envelope and you should consider double bagging the package
- Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't copy previous letters. Double check that the letter and papers are for the correct recipient and address
- When using a mailshot or multiple mailings, have a procedure in place to check that any personal information has not been included in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch
- Consider using signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery
- Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt
- If post goes astray or is issued to the incorrect address, notify a Data Protection Champion immediately and if the information contains personal or confidential information, the incident should be reported via the Data Breach procedure detailed in the LT2 Data Protection Policy

4.2 Email and other Electronic Communications

- LT2 does not have total control over emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources (such as emails ending in '.exe'). Employees should not click on links in emails unless they are from a trusted source and never provide passwords in response to email requests. Staff must inform the Trust Strategic IT Manager if a suspected virus is received.
- If an employee is not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted
- If an employee sends an email containing personal data to an incorrect recipient, they must inform a Data Protection Champion at once (please see the LT2 Data Protection Policy for the full data breach procedure)
- Staff should check the email address is the correct one – there are staff with similar names and outlook contacts will also have external email contacts. Double check that the email is for the correct recipient before sending. If sending to a list/group of parents or others, send using 'blind copy' (bcc) so the recipients are not copied in to a large list. This especially applies to mailshots.
- Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;
  a. An approved encrypted email service is used (e.g. egress or the encryption tool in Outlook) , or
  b. The information is encrypted / password protected in an attachment, or
  c. The information is to be sent to an approved LT2 email address, e.g. the trust or a school within the trust
  d. The intended email address utilises the same server
- Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the GDPR. If a permanent record is required they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a

permanent filing system for pupil, parent or staff records. When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as records

- Confidential emails must not be forwarded to an employee's personal email account for private use

4.3 Telephone Calls

Employees should:

- Ensure that they verify who they are speaking to. It may be appropriate to call them back to verify their credentials
- If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office
- If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation
- If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information
- Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person
- On occasions where employees need to make urgent, short, personal telephone calls on trust telephones, 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.

4.4 Conversation

Staff should remember that even though they may be on trust premises there may be pupils and visitors around

- When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job
- Always consider surroundings and the proximity of others who may be able to hear in public places

4.5 Information Sharing / Processing

When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:

- If a service is commissioned with an external provider that needs confidential information to operate then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf of LT2 or has sole or joint responsibilities for the personal data with LT2. All staff involved in such data commissioning/sharing must be aware of the details of any existing information sharing agreements/contractual agreements and the obligations that it places on them
- If information has to be shared with another organisation on a regular basis for legal reasons then this should be done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager

5. Working Away from School

The purpose of this section is to ensure that information assets and information processing facilities, used to access personal and confidential information, are adequately protected with logical, physical and environmental controls.

This includes working away from the school, at home and use of own devices to access personal and confidential information.

- Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in school, on the phone, at home, en route to or from school or home, at meetings, conferences, etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end, or ensuring it is only in the hands of those authorised to keep it
- Take only the confidential papers/files needed and these should be kept out of sight in a bag, do not carry around loose or in clear folder
- Managers must ensure a log is kept of which confidential paper case files/records staff are taking from school and when they are returned
- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead
- Equipment/media taken off-site must not be left unattended in public spaces

- Keeping information in cars: do not leave any paper files or equipment (laptop/notebook) unattended in the car. In some cases it is permissible to lock some files in a car (for example, if an employee has moved between sites for a meeting). In these cases, they must be stored in the boot. Laptops/equipment must never be left in a car. Equipment/papers/files must never be left in a car overnight.
- When travelling, laptops must be carried as hand luggage
- Travelling by public transport: make sure to take all information and equipment when leaving. Be aware of conversations on mobile phone about personal and confidential information
- Use of Laptops: Only school issued devices may be used and these must be password protected. Do not write down passwords/pin numbers. Employees must not use the 'remember me' option to save user and password details on your their devices when accessing LT2 systems. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. Remember any confidential files opened may be downloaded before closing down your device, so delete them from 'downloads'. If files are not accessed directly (e.g. via OneDrive), then all confidential files must be stored and accessed locally via an approved encrypted media.
- Working at home: Store paper and equipment securely after use. Don't leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure. Don't leave any trust equipment or information in a car overnight at home, bring into the house and secure. Don't bin confidential information at home, bring back into an office for confidential waste disposal. Use strong security on a home WiFi connection.
- Either when working at home or in a public space, employees must utilise a VPN
- When in a public space staff must use a privacy screen

6. Premises

- All staff must wear their ID badge on school premises and report losses or thefts immediately to the Trust Strategic IT Manager and School Operations Manager
- Make sure that all visitors sign in and out at all times and disclose who they are coming to see. Visitors should be supervised at all times and display a visitor/contractor ID badge
- Staff should be encouraged to challenge anyone in the school if they do not know who they are, e.g. if they are not accompanied by a member of staff or they are not wearing an ID badge
- Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception if necessary
- Managers should ensure that all paper-based records and any records held on computers are adequately protected. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced
- Parents and others who do not want to discuss their private matters with a receptionist in a public area should be offered the opportunity to be seen elsewhere

7. Portable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across the trust. Portable media devices include, but are not limited to USB sticks or memory cards.

- Connection of non-trust supplied removable media devices to the trust computing infrastructure is only permitted for the purpose of reading files from the device
- Trust files must not be written to a non -supplied device
- Staff must not alter or disable any controls applied to any computing device by IT Staff as part of the deployment of a removable media device
- Removable media devices must not be used for the primary long-term storage of trust information
- All information classified as 'LT2 MAT Confidential' or 'personal' that is stored on a removable media device must be encrypted
- Passwords applied to encrypted devices must conform to the minimum standard required stated in section 2.4

8. Access Control

- Access to information shall be restricted to users who have an authorised need to access the information. Users of information will have no more access privileges than necessary to be able to fulfil their role
- All requests for access to trust computer systems must be via a formal request to the Headteacher or CEO for approval
- The trust reserves the right to revoke access to any or all of its computer systems at any time
- Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources
- Users must not allow anyone else to use their account or use their computers while logged in with their account
- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended
- Users should not leave workstations or devices in 'sleep mode' for convenience

9. Monitoring System Access and Use

The purpose of this section is to establish control requirements for the monitoring and logging of information security related events relating to the use of LT2's information and information systems.

There will be regular reviews and audits of the safety and security of school technical systems

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. 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 Trust Strategic IT Manager and are kept for no longer than necessary. The trust will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy.

It is not the Trust's policy, as a matter of routine, to monitor an employee's use of e-mail service or 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 authorising 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.

Any monitoring will be undertaken in accordance with the Human Rights Act and any other applicable law.

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

More information relating to systems monitoring can be found in the LT2 Monitoring Policy.

10. Potential breaches of security and confidentiality

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it immediately to the relevant data protection champion and headteacher/CEO immediately.

For losses of equipment or if an employee may believe that email or the network may be at risk, they must contact the Trust Strategic IT Manager (rfsshelpdesk@rugbyfreesecondary.co.uk) immediately. If equipment or confidential information has been stolen report to the Police and obtain a crime reference number.Use the trust data breach procedure to report and record incidents. This procedure can be found in the Data Protection Policy.

11. Breaches of this Policy

Reasonable personal use is permissible provided it is in full compliance with the Trust's rules, policies and procedures. Misuse trust systems and breaches of this 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 email 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 as described in this policy.

Any such action will be treated very seriously and in accordance with the steps set out in this section 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.

Generally, 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.

11.1 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.

11.2 Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of noncompliance 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

11.3 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 wilful 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.