The 3-18 Education Trust

Information Security Policy and Procedure

Every individual is in a great school.

Approved: Autumn Term 2023

www.318education.co.uk

Contents

Introduction

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The 3-18 Education Trust (Trust) is dedicated to ensuring the security of all information that it holds and implements the highest standards of information security to achieve this. This document sets out the measures taken by the Trust to achieve this, including to:

- Protect against potential breaches of confidentiality.
- Ensure that all information assets and IT facilities are protected against damage, loss or misuse.
- Support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data.
- Increase awareness and understanding at the Trust of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

The Trust's trustees, local governors, employees, contractors, and volunteers (staff) are referred to the Trust's Data Protection Policy, Data Breach Policy and Online safety Policy for further information. These policies are also designed to protect personal data.

This policy and procedure applies to all staff and any and all third parties authorised to use the Trust's IT systems.

All staff are required to familiarise themselves with the content of this policy and procedure and to comply with the provisions contained within it. Breach of this policy and procedure will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy to remain compliant with legal obligations.

Definitions

Information

Information includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Trust, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

Information Security

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

Mobile Devices

For the avoidance of doubt, the term ‘mobile devices’ used in this policy and procedure refers to any removable media or mobile device that can store data. This includes, but is not limited to laptops, tablets, digital cameras, memory sticks and smartphones.

General Principles

All data stored on the Trust’s IT Systems are to be classified appropriately including, but not limited to personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the Trust’s Data Protection Policy. All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the IT Department the appropriate security arrangements for the type of information they access in the course of their work.

All data stored within the Trust’s IT Systems and paper records shall be available only to staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired and upgraded following authorisation by the IT Director or by such third party/parties as the IT Director may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including but not limited to the security, integrity and confidentiality of that data) lies with IT Director unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to IT Director / School’s Business Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day or when staff leave their desk unoccupied, all paper documents with personal information, sensitive personal information and confidential information shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use. If an individual does not feel there is appropriate and/or sufficient storage available, they must inform the School’s Business Manager as soon as possible.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. Particular care must be taken if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If an individual finds the security to be insufficient, they must inform the School's Business Manager as soon as possible. Increased risks of vandalism and or burglary shall be considered when assessing the level of security required.

The following measures are taken by the Trust to ensure physical security of the buildings and storage systems:

- Schools carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.
- Schools have an intercom system to minimise the risk of unauthorised people from entering the school premises.
- Schools close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.
- Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Trust IT and Digital Devices

The IT Director and IT Manager shall be responsible for the following:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with the Trust's security requirements;
- ensuring that IT Security standards within the Trust are effectively implemented and regularly reviewed, working in consultation with the Trust's and School's management and reporting the outcome of such reviews to the Trust's and School's management;
- ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations and other relevant rules whether now or in the future in force, including but not limited to the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the on-site School IT Support Technician shall be responsible for the following:

- assisting all members of staff in understanding and complying with this policy;
- providing all members of staff with appropriate support and training in IT security matters and use of IT Systems;
- ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities and any special security requirements;
- receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Data Protection Officer;
- taking proactive action, where possible, to establish and implement IT security procedures and to raise awareness among members of staff;
- monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Use of Trust Digital Systems

All staff must comply with the following when using the Trust's IT Systems.

- Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.
- Staff must immediately inform the IT Director, IT Manager or School Business Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Procedure.
- All Staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from IT Director and IT Manager 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. This permission must clearly state which software is permitted and onto which computer(s) or device(s) it may be installed. The IT Manager will only install software where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject. Where consent is given, all files and data should always be virus checked before they are downloaded onto the Trust's systems.
- Prior to any usage of physical media (e.g., USB memory sticks or disks of any kind) for transferring files, staff must ensure the physical media is virus scanned. Approval from the IT Manager must be obtained prior to transferring of files using cloud storage systems.
- If staff detect any virus this must be reported immediately to the IT Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

Digital Access Security

All Staff are 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 Trust IT staff to fulfil actions outlined in this policy.

The Trust has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Trust's network. The Trust also teach individuals about online safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

Passwords:

- All passwords must, where the software, computer, or device allows:
  - be at least 7 characters long including both numbers and letters;
  - cannot be the same as the previous 24 passwords staff have used;
  - not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.)
  - Must be protected by two factor or multi factor authentication (2FA/MFA) when required
- Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the School's Senior Leadership Team who will liaise with the IT Director or IT Manager as appropriate and necessary. Any Staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the Trust's Disciplinary Policy and Procedure. Any Staff who logs

on to a computer using another Staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

- If a password is forgotten the School IT Support Technician should be notified to have access to the IT Systems restored. A new password must set up immediately upon the restoration of access to the IT Systems.
- Passwords should not be written down if it is possible to remember them. If necessary, passwords may be written down provided they are stored securely (e.g., in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) will be protected with a screen lock that will activate after a period of inactivity. This time period or disable the lock must not be altered.

All mobile devices provided by the Trust shall be set to lock, sleep or similar after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. This time period must not be altered.

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.

Data Security

Personal data sent over the Trust network will be secure by means of access control in order to comply with the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Staff may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's dedicated Wi-Fi SSID provided staff follow the School's requirements and instructions governing this use. All usage of staff's own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The IT Director may at any time request the immediate disconnection of any such devices without notice.

Electronic Storage of Data

No data should be stored electronically on physical media and in particular personal data.

Staff should not store any personal data on any mobile device, whether such device belongs to the Trust or otherwise without prior written approval of the IT Director/Headteacher. Staff should delete data copied onto any of these devices as soon as possible and make sure it is stored on the Trust's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day and is done by IT Director.

Only Microsoft One Drives associated with user accounts and libraries within Microsoft SharePoint (associated with Trust or School provided user accounts) are to be used to access, store and share files.

Homeworking/Working away from Trust Offices

Personal or confidential information should not be removed from the Trust without prior permission from Headteacher/Deputy CEO/CEO/HR Director/IT Director/CFO except where the removal is temporary and necessary. When homeworking, permission will only be granted when appropriate technical and practical measures are in place within the staff's home to maintain the continued security and confidentiality of that information.

When such permission is given all reasonable steps must be taken to ensure that the integrity of the information and the confidentiality are maintained. Staff should ensure that the information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g., waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g., in car boots, cafes, etc.)

When homeworking, staff must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or in the case of electronical material, securely destroyed as soon as any need for its retention has passed.

Communications, Transfers, Internet and Email Use

When using the Trust's IT Systems, staff are subject to and must comply with the Trust's Online Safety Policy and Procedures.

The Trust work to ensure the systems protect Staff and pupils and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the School Business Manager or, for pupils, Designated Safeguarding Lead.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the Trust cannot accept liability for the material accessed or its consequence.

All personal information and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery. Postal, DX, fax and email addresses and numbers should be checked and verified before staff send information to them. In particular extra care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

Care should be taken to maintain confidentiality when speaking in public places.

Staff should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the IT Director/School Business Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the IT Director/School Business Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue and shall take all steps necessary to respond to the issue.

Staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the IT Director/School Business Manager. Any attempt to resolve an IT security breach by Staff must be under the instruction of and with the express permission of the IT Director/School Business Manager.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to IT Director/School Business Manager.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.

Links to other Policies and Procedures

Data Protection Policy and Subject Access Request Procedure
Data Breach Procedure
Operation of CCTV Procedure
Protection of Pupils Biometric Information and Consent to use Biometric Data
Records Management Policy and Retention Schedule

Procedure Monitoring and Review

Monitoring

The Chief Executive Officer, in conjunction with the IT Director and DPO, will monitor the outcomes and impact of this procedure on a 2 yearly basis and whenever new equipment is introduced.

Review

Member of Staff Responsible	Chief Executive Officer
Relevant Guidance/Advice/Legal Reference	UK General Data Protection Regulation Data Protection Act 2018
Procedure Adopted By	Trust Board
Date of Policy	Autumn Term 2023

Review Period	Two Yearly
Date of Next Review	Autumn Term 2025