Information Security Policy

Policy Information	
Policy Owner	Chief Operating Officer
Issue Version	V1
Approving Committee	F&A Committee
Adopted Date	June 2021
Review Cycle	Bi-Annual
Last Review Date	June 2021
Next Review Date	June 2023

Adoption of the Policy

This Policy has been adopted and reviewed by the Trustees of Transforming Futures Trust

Signed **Date: June 2021**

(Chair of Trust)

Version Control Amendments

Version No	Date	Summary of Changes

1. Introduction

This Policy sets out the Framework for ensuring Trust Information is managed, processed and stored securely in a manner which is legally compliant.

Any member of staff found to have violated this policy may be subject to disciplinary action, under the Trust HR Disciplinary Policy up to and including termination of employment. Any exceptions to the policy must be pre-approved by the CEO.

2. Legal Framework

The Trust has a legal duty to comply with the UK-GDPR, as well as Data Protection Act 2018, Privacy and Electronic Communications Regulations 2019 (PECR).

3. Aims

The aim is to ensure that all staff are aware of the principles of the CIA Triad when dealing with information and use the principles from their day-to-day handling of information up to the development and adoption of new ways and systems designed for handling information.

The CIA Triad Principles are:

Confidentiality

Information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity

Maintain the accuracy and completeness of data over its lifecycle.

Availability

Information must be available when needed and appropriate means of access or disclosure must be understood.

Adoption of this concept will reduce the risk of harm to individuals, reduce the vulnerability of the organisation and the likelihood of financial penalties that may be given by supervisory authorities such as the Information Commissioner's Office (ICO).

4. Roles and Responsibilities

Information Security Lead

Accountability for Information Security rests with the the CEO. The Information Security Lead delegates the function to the Chief Operating Officer and the technical support is provided through Delt Services Ltd.

Such activities include:

- Development of localised guidelines for the use of specific systems, training plans, threat awareness and updates, spot checking and auditing.

Governance of Information Security is overseen by the Trust Finance and Audit Committee.

Data Protection Officer (DPO)

The Trust DPO is outsourced and is responsible for supporting the Trust's compliance with Data Protection legislation. The current Trust DPO provider is at GDPR - Transforming Futures Trust.

Headteachers

Headteachers are primarily responsible for ensuring the security of their physical environments where information is processed or stored. They are also responsible for ensuring:

- Staff are aware of Trust IT and GDPR policies,
- IT access is controlled through the HR starters and leavers process,
- Staff abide by the Trust IT and GDPR policies in their work environment and in how they undertake their roles.
- Ensuring that staff have taken part in the relevant and adequate training when available.

IT Team

The IT Team whether on-site or through a third-party contract must:

- ensure that all network, mobile devices, and removable media assets are securely controlled and managed. This includes maintaining appropriate storage facilities, producing and reviewing guidance regarding the safe storage and use of assets, user access agreements and user access control, such as the removal of users when informed to do so by managers, or under exceptional circumstance.
- Ensure the appropriate maintenance of software in use by the Trust. This includes software patching routines, application or alterations or the removal of software considered to be vulnerable, the assessment of such levels of vulnerability, and the notification to all relevant staff of existing threats, emergent threats, and appropriate safe use.
- Oversee the development and implementation of new technologies to build safe and secure systems, in agreement with the Information Security Lead.

Information Owners/Responsible Persons

The approach to the use of data will determine who Information Owners are. In general, the ownership or responsibility will fall to the person who retains and uses the information within their workspace, for example the Lead Administrator will own the data used within the academy offices, including centralised pupil information; the Designated Safeguarding Lead (DSL) will own Safeguarding Information; and individual teachers will own class lists and pupil information where it is not held on the Pupil Information Management System.

Information Owners are responsible for managing the accuracy and security of their data. Owners will also need to discuss with the Information Security Lead and DPO the implications of using third parties to process information or when sharing information. Where this includes personal data or other sensitive information, appropriate agreements must be in place.

All Employees and External Individuals

Everyone is responsible for Information Security and should be aware of and understand the requirements of on them in line with this Policy and any associated guidance.

The key points for all employees to remember are:

- What information they are using, and how it should be handled, stored, or destroyed.
- What procedures, standards and agreements exist for the sharing of information with others.
- How to report breaches.
- Their responsibility for raising their concerns with their manager, the relevant Information Owner, DPO or Information Security Lead.

Individuals who may work in the Trust.

Individuals who may work in the Trust, such as IT consultants, auditors or external agencies, must be able to demonstrate their organisation's Information Security approach or have an appropriate confidentiality statement within their work description.

They are made aware of what they should do if they inadvertently access information that they should not have done or discover a breach. This may be as simple as letting them know to contact the person who is responsible for them or making them aware of who the relevant manager is that they can report to.

5. Specific Security Requirements

Contracts of Employment

Staff suitability are assessed at all points of employment, in line with safer recruitment policies and guidance, and all employee contracts contain reference to confidentiality. Information in the form of the ICT Acceptable Use Policy and the GDPR Policy.

Access Control

Information is restricted to only those who have an acceptable business reason to access such information. Passwords or emergency access without authorisation may only be made in exceptional circumstances and the decision to do so must be relayed to the Information Security Lead at the earliest possible point.

Computer Access Controls

Access to computer systems is managed by the IT Team. A form of system monitoring is in place that can be used to determine who accessed which device and at what time. The fundamentals of password security are in place to ensure that passwords are not shared which would result in misidentification with the exception of the point regarding emergency access.

Account Management

New IT Accounts are created by the IT Team upon receipt of a new starter form, which is signed by the Headteacher or a member of the Trust executive Team. Any changes to access levels would need the same sign off. Subsequently accounts are removed following the leavers process.

Application Access Controls

Specific applications are administered effectively by the IT Team. When adopting a new application, a proper assessment of access controls are made and, if necessary, locally produced guidelines regarding its use are made. This may be covered as part of the Data Protection Impact Assessment.

Equipment Security

Information may be stored in physical containers such as filing cabinets, draws, safes and storage rooms. It will in most cases be retained electronically, however the principles of security are the same.

Any area where information is stored is secured in a manner appropriate to the type and sensitivity of information stored within, for example sensitive financial records, safeguarding records and HR records must be secured by lock, or if stored electronically on a secure section of the computer network isolated by specific permissions.

General lists and necessary contact details are stored out of sight in line with a clear desk routine, or, if stored electronically, may be stored in a general open section of the computer network. In cases where highly sensitive information is stored electronically, it is encrypted wherever possible.

Mobile Devices & Removable Media

Removable media must not be used on the IT network, as even when this is encrypted, there is a high risk of it being lost or stolen.

Mobile devices must be issued by the Trust to ensure they are suitably encrypted and can be effectively monitored on the network.

Mobile phones owned by staff can be used, however they must not be used to take photos or videos of children and only used for managing and monitoring emails and applications. The Trust Outlook cannot download onto a staff owned mobile device without the IT team approving access from checking the devices security features being suitable.

Computer Network Procedures

The arrangement and control of the computer network is documented.

Remote Access

Staff must not email or share files or folders onto their own devices to work on at home. For staff needing to work from home, remote access is provided through a secure portal that can only be used from a Trust device.

Data Back-Ups

The Trust backs-up data regularly and separately from the location of the data.

Back Ups

- All drives backup on the hour, all day, these are retained for 24 hours
- Then 1 Recovery point per day for 7 Days

Retention

- OFF SITE SCHEDULE and RETENTION
- Replication Offsite happens continuously throughout the day
- All drives backup on the hour, all day, these are retained for 24 hours
- Then 1 Recovery point per day for 7 Days

Disposal of IT, AV and Digital Equipment supplied by the Trust.

Disposal of this type of equipment is governed by the WEEE directive and the Trust has clear guidelines that must be followed.

The disposal of all such equipment is arranged of by the Trust IT Helpdesk, who will ensure that all legislation is followed and equipment disposed of securely and safely, using a contractor who will dispose of the equipment in accordance with the required legal standard.

Password Protocol

Passwords are the front line of protection for user accounts. They are used to authenticate each user. A poorly chosen password may result in the compromise of the Trust's entire network and data. As such, all Trust staff are responsible for taking the appropriate steps, as outlined in this document, to select and secure their passwords.

Strong passwords have the following characteristics:

a. They must be at least 8 digits long to comply with our Cyber Security Certification.
b. They must contain both upper and lower case characters (e.g., a-z, A-Z).

c. Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,/ - where allowed by the system.

d. Not be based on personal information, names of family, etc.

All passwords are to be treated as sensitive, confidential Trust information. This information must not be shared with anyone. The following must always be followed in terms of password management:

- Passwords must never be written down, stuck to a workstation screen or in a desk drawer, written in clear text in a planner, or stored on-line in clear text.
- Passwords must not be revealed in email messages.
- A different password to be used for each application/system.
- If an account or password is suspected of being compromised, report the
- Re-using passwords must be avoided.

6. Incident Management Process

GDPR Breach

For a GDPR personal data breach, the Chief Operating Officer is informed via the breach being reported through the GDPRiS system. The Chief Operating Officer undertakes the role of investigating officer and informs the DPO for advice and guidance. A Breach Investigation Form is completed and uploaded to the GDPRiS system as a record of the activities undertaken. Where the breach has the potential for the ICO to be informed the Trust IMT process will be instigated as per the Trust Business Continuity Plan.

IT Information Security Breach

Staff report IT information security breaches, via the IT helpdesk. These are escalated to the Chief Operating Officer for information. Where the breach is assessed as a risk that has the potential for the ICO to be informed, the Trust IMT process will be instigated as per the Trust Business Continuity Plan.

7. Insurance

The Trust is part of the RPA Cyber Insurance Pilot provided by the DfE. Cyber Insurance has been provided free of charge for 1 year following the successful completion of the Cyber Essentials Accreditation.