Information Security Policy

Person Responsible	Rob Knott
Approved by Directors	March 2020 / ratified by directors July 2023
First Written	February 2020 / updated July 2023

For Review	Reviewed	Signature
July 2021	Amended with Judicium content	Rob Knott and Jo Ronxin
July 2022	Completed	Jo Ronxin and Karen Bannister
July 2023	Amended/Completed	Rob Knott
July 2024	Completed – no change	Rob Knott and Karen Bannister
July 2025		
July 2026		

All policies are renewed annually. If no change then just signed.
If an amendment or full change is required, this is recorded.

Definition: Setting

A Setting is any central Trust department, early years or school provision with Acorn Education Trust.

Acorn Education Trust (the Trust) is committed to safeguarding the privacy and rights of individuals whose data is obtained, stored, processed, or supplied. In accordance with the UK General Data Protection Regulation (UK GDPR), the Trust upholds strict standards of information security to ensure the protection of all data under its control.

This document outlines the measures implemented by the Setting to achieve this objective, including:

a) **Confidentiality Protection:** The Trust takes proactive steps to prevent any potential breaches of confidentiality. Stringent measures are in place to restrict unauthorised access, alteration, disclosure or destruction of personal data.

b) **Safeguarding Information Assets and IT Facilities:** The Trust ensures that all information assets and IT facilities are effectively protected against any form of damage, loss, or misuse. Robust security controls and protocols are in place to mitigate risks and maintain the integrity of data.

c) **Compliance with Data Protection Policy:** The Trust actively supports its Data Protection Policy, which ensures that all staff members are well-informed and compliant with UK laws and internal procedures regarding data processing. Regular training and awareness programs are conducted to promote understanding and adherence to these regulations.

d) **Enhancing Information Security Awareness:** The Trust places great emphasis on increasing awareness and understanding of information security requirements within its educational settings. Staff members are educated about their responsibility to safeguard the confidentiality and integrity of the information they handle, further fostering a culture of information security.

By implementing these measures, the Trust strives to create a secure environment for data processing, promoting privacy and protecting the rights of individuals.

Introduction

Information security is of paramount importance in safeguarding the confidentiality, integrity, and availability of information and information systems. It encompasses measures to prevent unauthorised access, use, disclosure, disruption, modification or destruction of data.

To ensure adherence to information security principles, the Trust has established comprehensive policies, including the Data Protection Policy and Data Breach Policy. These policies are designed to protect personal data and can be accessed on the Acorn Education Trust website.

It is important to clarify that in this policy, the term "mobile devices" refers to any portable media or device capable of storing data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks, and smartphones.

Scope

This policy applies to all information, regardless of its form (written, spoken, or electronic), that is handled, used, or transmitted by or on behalf of the Setting. It encompasses data stored on computer systems, paper records, handheld devices, and information communicated verbally.

All individuals, including staff members, temporary workers, contractors, volunteers, governors, and authorised third parties using the IT systems, are bound by this policy.

It is mandatory for all staff members to familiarise themselves with the policy's contents and comply with its provisions. Failure to comply will be considered a disciplinary offence and appropriate disciplinary action will be taken in accordance with the Trust's Disciplinary Policy and Procedure, which may include summary dismissal based on the severity of the breach.

This policy does not constitute a contractual obligation or form part of any individual's terms and conditions of employment within the Setting and is not intended to have contractual effect. The policy will be regularly reviewed to ensure compliance with evolving data protection legislation, and necessary amendments will be made to maintain legal compliance.

General principles

All data stored within our IT systems must be appropriately classified, including personal data, sensitive personal data, and confidential information, among others. For more information on data categories, please refer to the Trust's Data Protection Policy and Record of Processing Activities. It is essential to handle data in accordance with its classification.

Staff members should consult with the Trust's Head of IT to determine the suitable security measures for the specific information they access during their work.

Access to data stored on the Setting's IT systems and paper records should be limited to staff members with a legitimate need for such access. Adequate measures must be implemented to prevent unauthorised access, processing, loss, or corruption.

The installation, maintenance, servicing, repair, and upgrading of all IT systems should be conducted by the Trust or by authorised third parties approved by the Trust's Head of IT.

The responsibility for the security and integrity of all IT systems and the data they contain, including but not limited to security, integrity and confidentiality of the data, lies with the Trust unless explicitly stated otherwise.

All staff members have a duty to report any actual or potential breaches of data protection compliance to the Trust's GDPR Managers, who will conduct an investigation. Any breach involving personal data or sensitive personal data, whether known or suspected, must be reported to the Data Protection Officer (details of the officer can be found in our Data Protection Policy).

Physical security and procedures

To safeguard paper records and documents containing personal, sensitive and confidential information, the following measures shall be implemented:

Positioning and Secure Storage:

- Paper records should be positioned in a way that minimises visibility to passers-by, such as avoiding placement near windows;
- At the end of the working day or when leaving the desk unoccupied, all paper documents must be securely locked away to prevent unauthorised access;
- Available locked cabinets and storage systems should be utilised to store paper records when not in use.

Restricting Access and Usage:

- Paper documents containing confidential personal information should not be left unattended on office or classroom desks, staffroom tables, or noticeboards accessible to the general public, unless there is a legal requirement or relevant consents have been obtained;
- Exercise caution when documents need to be taken outside the Setting.

Physical Security Review and Maintenance:

- Regular reviews of the physical security of buildings and storage systems should be conducted;
- If you identify insufficient security measures, promptly inform the Trust's site team;
- Assess the level of security required considering increased risks of vandalism or burglary.

Building Maintenance and Access Control:

- The settings conduct regular checks to ensure buildings and storage systems are well-maintained;
- An intercom system or similar access control mechanisms are in place to minimize the risk of unauthorised individuals entering the Setting's premises;
- Setting gates are closed during specific hours to prevent unauthorised access to the building;
- Alarms, where installed, are set nightly;
- CCTV cameras are deployed at certain settings and monitored by the Trust's site team.

Visitor Management:

- Visitors should be required to sign in at the reception;
- Visitors should always be accompanied by a staff member and never left alone in areas where they could access confidential information.

<u>Computers and IT</u>

Responsibilities of the Head of IT and IT team:

The Head of IT and the IT team have the following responsibilities:

- Assessing and ensuring the suitability of all IT systems for compliance with the Setting's security requirements;
- Effectively implementing and regularly reviewing IT security standards within the Setting in consultation with management and reporting the outcomes of these reviews to management;
- Keeping all staff members informed about this policy and relevant legislation, regulations and rules, including the UK GDPR and the Computer Misuse Act 1990.

In addition, the Trust's IT team is responsible for:

- Assisting all staff members in understanding and adhering to this policy;
- Providing appropriate support and training to staff members regarding IT security matters and the use of IT systems;
- Granting appropriate levels of access to IT systems based on each staff member's job role, responsibilities and any special security requirements;
- Receiving and handling reports related to IT security matters and taking necessary action in response (including informing the Data Protection Officer if the reports involve personal data);
- Proactively establishing and implementing IT security procedures and raising awareness among staff members;
- Monitoring IT security within the setting and taking necessary action to implement this policy and any future changes to it;
- Ensuring regular backups of all data stored within the IT systems are performed at scheduled intervals and securely stored.

The Trust's IT team plays a crucial role in maintaining the security and integrity of IT systems and supporting staff members in their use of these systems.

Responsibilities – Members of staff

All members of staff are required to adhere to the provisions outlined in this policy when using the IT Systems:

- To ensure the security of information and prevent accidental loss or disclosure, it is essential to lock computers and other electronic devices when they are not in use;
- If you identify any security concerns that could potentially result in a data breach, it is your immediate responsibility to notify the Acorn IT team as specified in the Data Breach Policy;
- In the event of any technical issues, including hardware failures or software errors, occurring on the IT Systems, it is crucial to report them promptly to the Trust's IT team;
- Installing personal software on the IT Systems is not permitted without the approval of the Trust's Head of IT. Any software owned by you must undergo the necessary approval process by the Trust's Head of IT. Installation of approved software should pose no security risks to the IT Systems and must not violate any license agreements;
- If you detect any viruses, it is imperative to report them immediately to the Trust IT team, even if the anti-virus software automatically resolves the issue.

By adhering to these responsibilities, you contribute to maintaining a secure IT environment within Acorn Education Trust.

Access security

All members of staff have a responsibility to ensure the security of the equipment allocated to or used by them, ensuring that it is not used by anyone in violation of this policy.

To safeguard the Setting's network, a secure firewall and anti-virus software are in place, preventing unauthorised access. Additionally, individuals are educated on e-safety to promote awareness and protection of the Setting's network and personal well-being.

All IT Systems, especially mobile devices, must be protected with a secure password, passcode or other approved secure log-in method as determined by the IT Department. Biometric log-in methods can only be used with IT Department approval.

Passwords must adhere to the following criteria where the software, computer, or device allows:

- Be a minimum of 6 characters long, including both numbers and letters;
- Be changed regularly, at least every 180 days;
- Not be the same as any of the previous 10 passwords used;
- Avoid obvious or easily guessable combinations, such as birthdays or memorable names.

Passwords must be kept confidential and not shared with others unless authorised by a member of the Senior Leadership Group, who will coordinate with the Head of IT as necessary. Disclosing passwords without authorisation may result in disciplinary action in accordance with the Trust's Disciplinary Policy and Procedure. Logging onto a computer using another staff member's password is considered a serious violation and may result in disciplinary action, including summary dismissal for gross misconduct.

In the event of forgetting a password, staff should notify the Trust IT team to restore access to the IT Systems. It is mandatory to set up a new password immediately upon regaining access. Whenever possible, passwords should be memorised and not written down. If necessary, securely store written passwords in a locked drawer or a secure password database, never leaving them on display for others to see.

Computers and electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen) must be protected with a screen lock that activates after a period of inactivity. The time period and lock settings must not be altered or disabled.

All mobile devices provided by the Trust must be configured to lock, sleep, or activate a similar security feature after a period of inactivity. Unlocking or waking the device should require a password, passcode or other authorised log-in method. The time period for this feature should not be modified.

Staff should be aware that failing to log off and leaving computers unattended may result in being held accountable for any unauthorised activities conducted by another user on their computer, which would violate this policy, the Trust's Data Protection Policy and the confidentiality requirements for certain information.

Data security

To ensure the security of personal data, all data transmitted over the Setting's network will be appropriately encrypted or secured.

Staff members are strictly prohibited from downloading, installing, or running software from external sources without obtaining prior authorisation from the Trust IT Team. This includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown sources. In cases where authorisation is granted, all files and data must undergo virus scanning before being downloaded onto the Trust's systems.

If you wish to connect your personal devices, such as laptops, tablets, or smartphones, to the Setting's Wi-Fi, you must adhere to the requirements and instructions provided by the Trust's IT team. Please note that all usage of personal devices while connected to the Setting's network or any other part of the IT Systems is subject to all relevant Trust policies, including this policy. The Trust's IT team reserves the right to request the immediate disconnection of any personal devices without prior notice.

Electronic storage of data

To ensure the security of electronic data, the following guidelines should be followed:

- Portable data, especially personal data, must be stored on encrypted drives using methods recommended by the Trust's IT team;
- Data stored electronically on physical media, especially personal data, should be securely stored in a locked box, drawer, cabinet or similar;
- Personal data should not be stored on any mobile device, regardless of whether it belongs to the Setting. If data is copied onto these devices, it should be promptly deleted and stored on the Setting's computer network for proper backup purposes;
- It is essential that all electronic data is securely backed up by the end of each working day to prevent data loss and ensure data integrity.

By adhering to these guidelines, we can protect sensitive information and maintain the security of electronic data storage within the Trust.

Home working

When working from home, it is essential to maintain the security and confidentiality of information. Therefore, the following guidelines should be followed:

- Confidential or other sensitive information should not be taken home without prior permission from the Trust's IT team. Permission will be granted only when appropriate technical and practical measures are in place at your home to ensure the continued security and confidentiality of the information.
- If you have been authorised to take confidential or sensitive information home, it is your responsibility to ensure its security. This includes:

    - Keeping the information in a secure and locked environment where it is inaccessible to family members or visitors;
    - Properly disposing of all confidential material that is no longer needed. Paper-based material should be shredded, and electronic material should be securely destroyed.

By adhering to these guidelines, we can ensure the protection of confidential information and maintain the security and integrity of data while working from home within the Trust.

Communications, transfer, internet and email use

The Trust is committed to maintaining secure and effective communication systems for the protection of pupils and staff. Our systems undergo regular review and improvement to ensure their reliability and security.

If staff or pupils come across any inappropriate websites or materials, it is important to report them promptly to the Trust's IT Team. By doing so, we can take necessary actions to address and prevent access to unsuitable content.

The IT team conducts regular checks to ensure that our filtering methods are appropriate, effective, and reasonable, aiming to provide users with access to suitable materials. However, it is important to acknowledge that complete guarantee of access to only appropriate content may not always be possible. Therefore, the Setting cannot accept liability for the material accessed or its consequences.

When sending personal information, especially sensitive or confidential data, it should be encrypted before transmission via email or sent using tracked DX (document exchange) or recorded delivery methods. Fax transmission should be avoided unless you can ensure that it will not be inappropriately intercepted at the recipient's fax machine.

Before sending information, it is essential to verify the accuracy of postal, DX, fax, and email addresses and contact numbers. Particular caution should be exercised with email addresses, as auto-complete features may occasionally insert incorrect addresses.

Maintaining confidentiality is crucial when discussing sensitive matters in public places. Care should be taken to ensure that confidential information is appropriately marked as "confidential" and only shared with those individuals who require access to the information for their work within the Setting.

Personal or confidential information should not be taken from the Setting without prior permission from the Trust, except when temporary and necessary. If such permission is granted, it is your responsibility to take reasonable steps to maintain the integrity and confidentiality of the information. This includes:

- Ensuring that the information is not transported in transparent or unsecured bags or cases;
- Avoiding reading the information in public places, such as waiting rooms, cafes, trains, etc.;
- Never leaving the information unattended or in any place where it may be at risk, such as car boots or cafes.

By following these guidelines, we can ensure the secure and appropriate handling of communications, transfer, internet use, and email within the Trust.

Reporting security breaches

The Trust recognises the importance of promptly addressing any concerns, questions, suspected breaches or known breaches related to data protection. Therefore, all such incidents should be immediately referred to the Trust's GDPR Managers. It is the responsibility of all staff members to report any actual or potential data protection compliance failures they encounter.

Upon receiving a question or notification of a breach, the GDPR Managers will swiftly assess the issue, including evaluating the associated level of risk. They will take all necessary steps to respond appropriately and effectively to the situation.

Under no circumstances should staff members attempt to resolve an IT security breach independently without first consulting the Trust's GDPR Managers. If a staff member is directed and granted explicit permission by the GDPR Managers, they may participate in the resolution process.

In the event of missing or stolen paper records, mobile devices, computers or physical media containing personal or confidential information, immediate reporting should be made to both the Trust's IT team and GDPR Managers.

It is crucial that all IT security breaches are thoroughly documented, providing comprehensive details of the incident. The Data Breach Policy outlines the specific procedures and guidelines for notifying data breaches.

Related Policies

Staff members should refer to the following policies that are relevant to this information security policy:

- Data Breach Policy
- Data Protection Policy

By adhering to these policies, we can ensure a proactive approach to reporting and addressing security breaches within the Trust.