IT Security Policy

This policy is prescribed by The Good Shepherd Trust and all reference to 'the Trust' includes all Trust schools, the central team and subsidiary organisations.

Date adopted:	01/04/2024	Last reviewed:	01/04/2024
Review cycle:	2 years	Is this policy statutory?	No
Approval:	CEO	Author:	COO
Next Review Date:	01/04/2026		

Revision record

Minor revisions should be recorded here when the policy is amended in light of changes to legislation or to correct errors. Significant changes or at the point of review should be recorded below and approved at the level indicated above.

Revision No.	Date	Revised by	Approved date	Comments
1	10/03/2024	L Mason	01/04/2024	This policy combines previous policies: Acceptable Use, Access Control, Electronic Information Systems and Password Policy

1. Introduction

1.1. Employees at the Good Shepherd Trust (GST) access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. This policy provides a framework for how user accounts and privileges are created, managed and deleted. It includes how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorised privileges or access.

1.2. This policy applies to:

1.2.1. All school's workforce.

1.2.2. All central Trust staff.

1.2.3. Volunteers given access to Trust IT systems.

1.2.4. Third party organisations who require access to the Trust information systems.

2. Definitions

2.1. **Users -** This is the collective term used to describe all those who have access to the Good Shepherd Trust's information and information systems as outlined in the Scope of this policy.

2.2. **Privileged Users** - A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard users are not authorised to perform.

2.3. **Managers** are people responsible for managing or administrating a system or staff. They are responsible for ensuring that members of their team have the minimum levels of access to systems they need to perform their job. They must authorise the access rights for each individual team member and keep a record of the latest access permissions authorised. All Managers should review the access levels of their people to ensure they are appropriate.

2.4. **IT Support Team** are responsible for granting access to systems as described in local work instructions or use of Role Based Access Controls Matrix in accordance with the relevant procedures. IT Support Teams must evaluate and, if necessary, challenge authorised access to help identify any obvious anomalies in the access levels granted or requested.

3. User Responsibility

3.1. Users will only use their account and access in accordance with GST's Data Protection.

3.2. Compliance with this policy will be assessed regularly. Any violation of this policy must be investigated and may result in disciplinary action being taken.

3.3. Staff with access to Trust IT systems must undergo annual Cyber Security Training and GDPR refreshers as defined by the Trust.

3.4. Staff should make themselves aware of their local Cyber Incident Response plan available from their School Business Manager or Officer Manager.

4. User Access Account Management

4.1. User account management procedures must be implemented for user registration, modification and de-registration on all GST information systems. These procedures must also include processes for monitoring redundant and inactive accounts. All additions, deletions, suspensions and modifications to user accesses should be captured in an audit log showing who took the action and when. These procedures shall be implemented only by suitably trained and authorised employees.

4.1.1. Access controls must be allocated on the basis of business need and 'Least Privilege'. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

4.1.2. Users must only use business systems for legitimate use as required by their job and in accordance with the procedures for those systems.

4.2. All access to GST information systems must be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user's identity. Users will normally be asked for multi-factor authentication.

4.3. All changes to privileged accounts must be logged and regularly reviewed. Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organisation. Users' access rights will be reviewed at regular intervals no longer than annually.

4.4. On resignation of employment, line managers will undertake a risk assessment and determine whether existing access rights of an individual should be reviewed and reduced whilst working out their notice.

4.4.1. Hostile terminations will be communicated to system administrators immediately and access immediately disabled.

4.4.2. Managers will inform IT of the names of employees that will be leaving School/partner employment at least 48 hours before the end of their last working day. Access rights should be disabled by 5.00 pm on the employee's lasting working day.

4.4.3. It is the responsibility of the School Business Manager or Office Manager to ensure the return their devices of their last working day.

5. Network Access Control

5.1. An access management process for every system/database must be created, documented, approved, enforced and communicated to all relevant employees and partner organisations.

5.2. Each business application run by, or on behalf of the GST, will have a nominated system administrator who is responsible for managing and controlling access to the application and associated information.

5.3. The appropriate information, system, database, or application owner is the only individual that can authorise a systems administrator to grant or update access via the formal access management process.

5.4. The CFOO will ensure that there is sufficient monitoring of the process to ensure that access control is appropriately implemented by liaising with the IT support provider on a quarterly basis.

5.5. Special attention is given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

6. Passwords

6.1. Third Party providers may enforce even more stringent password requirements than are listed in this policy which should be adhered to. This policy is intended to define the minimum requirements that GST employees are to adhere to.

6.2. GST acknowledges that Passwords are only one part of an employee's cyber security responsibilities. Staff are expected to use multi-factor authentication when this is required by school systems. The Trust adheres to NCSC guidelines.

6.3. Password creation

6.3.1. All passwords should be reasonably complex and difficult for unauthorised people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. A combination of random words is the most secure and is easy to remember. For example: GreenTreeGarden17! Or 30Schoolbooks?

6.3.2. In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" or "J@net1965" are equally bad from a security perspective.

6.3.3. A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. recommended method to choosing a strong password that is still easy to remember.

6.4. Employees must choose unique passwords for all of their GST accounts and may not use a password that they are already using for a personal account.

6.5. If the security of a password is in doubt – for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.

6.6. Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must

be changed as quickly as possible.

6.7. Protecting passwords

6.7.1. Employees must never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

6.7.2. Employees must never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system without prior approval from the Trust Data Protection Officer or Senior Member of Staff if they are not available.

6.7.3. Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees must complete mandatory Data Protection and Cyber Security training on how to recognise these attacks.

6.7.4. Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

6.7.5. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

7. Equipment Security

7.1. All members of 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 in accordance with this policy.

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

7.3. 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.

7.4. Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the Principal School Leader or a member of the Senior Leadership Team.

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

7.6. Members of staff who have been issued with a laptop, iPad (or other mobile device tablet), must ensure that it is kept secure at all times, especially when travelling.

8. Systems Use and Data Security

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

8.2. All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the IT support provider 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.

8.3. No device or equipment should be attached to our systems without the prior approval of the IT Support Provider. This includes, but is not limited to, any PDA or telephone, iPad (or other mobile device tablet), USB device, digital camera, MP3 player, infra-red connection device or any other device.

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

9. E-mail etiquette and content

9.1. Staff are strictly prohibited from using the Trust's email facility for personal emails at any time.

9.2. 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. 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.

9.3. 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.

9.3.1. The Trust reserves the right to view work emails of employees at any time.

9.4. 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.

9.5. 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.

9.6. Staff should not send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

10. Use of the web and the internet

10.1. The Trust actively monitors internet usage of its staff and students. 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.

10.2. School senior leaders monitor usage through internet filtering reports on a weekly basis.

11. Inappropriate use of equipment and systems

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

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

11.3. Misuse of the internet may, in certain circumstances, constitute a criminal offence.

11.4. Misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
(b) transmitting a false and/or defamatory statement about any person or organisation;
(c) sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
(d) transmitting confidential information about the Trust and any of its staff, students or associated third parties;
(e) transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Trust;
(f) downloading or disseminating material in breach of copyright;
(g) copying, downloading, storing or running any software without the express prior authorisation of the IT support provider;
(h) engaging in online chat rooms, or online gambling;
(i) forwarding electronic chain letters and other materials;
(j) accessing, downloading, storing, transmitting, or running any material that presents or could present a risk of harm to a child.

11.5. Any such action will be treated very seriously and may result in disciplinary action.

Appendix 1: Example Access Control Permissions

Function/Role	Pupil Sensitive Information	Staff Information	Financial Data	H&S records and logs	School Website Editing	Notes
Head Teacher	x	x	x	x	x	
SENCO	x					
Teacher	x				x	
Administrator		x	x		x	
School Business Manager	x	x	x	x	x	
IT Support Provider		x*		x	x	*Only given temporary access when necessary authorised by a member of SLT.

This may have to be completed for each information system

Agreed by Date Next Review

Appendix 2: Example Access Control Log

Name of Staff Member	Old Role	New Role	Change to access	Agreed by	Date
Jane Doe	Teaching Assistant	Teacher	Increased access to pupil infomation	HT (signed)	1 Sept 2021
Bob Dylan	SENCO	Resigned	All Access removed	SBM (signed	1 Sept 2021