Access Control 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: 1 October 2021 Last reviewed: 30 August 2022
Review cycle: Every 2 years or earlier Is this policy statutory? No
Approval: COO Author: Data Officer
Local approval*: n/a Local author*: n/a
* Only for policy/procedures that are templates and require local adaptation. Local approval will either be the local committee, the head teacher, or the CEO (refer to policy schedule)

Revision record

Revision No.	Date	Revised by	Approved date	Comments
1	30/8/22	Data Officer	31/8/22	New Policy Template

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. The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the Trust Data Officer.

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

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. This includes a "standard user" with approved elevated privileges that allows equivalent access to that of a privileged user.

2.3. **Senior Responsible Owner (SRO)** SROs are responsible for ensuring that the requirements of this policy are implemented within any programmes, projects, systems or services for which they are responsible. The SRO is responsible for ensuring that a robust checking regime is in place and complied with to ensure that legitimate user access is not abused.

2.3.1. The SRO may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and associated checking regime.

2.3.2. Any non-compliance with this policy must be supported by a documented and evidence based risk decision accepted by the SRO.

2.4. **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.

2.5. **IT Support Teams** 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.

2.6. Users who are not explicitly granted access to GST information or information systems are prohibited from using such systems. Individuals employed by or under contract to the Trust shall be granted access only to information and information systems that are required to fulfil their duties.

2.7. Access to Trust systems will be granted only to those staff who have signed the School's Acceptable Use Policy (for School employees) and undergone Cyber Security and GDPR training as designated appropriate to their role by the Trust.

2.8. This policy applies to:

2.8.1. All school's workforce.

2.8.2. All central Trust staff.

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

2.9. Principle of Least Privilege

2.9.1. 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.

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

3. User Access Account Management

3.1. 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.

3.2. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.

3.3. 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 limited to only one user account for each individual information system for non-administrative purposes.

3.4. Any variations from this policy must be authorised by the Senior Responsible Owner (SRO). All users shall have a user ID for their sole use for access to all computing services. All individual user IDs must be unique for each user and never duplicated. All user accounts that have not been accessed for an agreed period, without prior arrangement, must be automatically disabled. All administrator and privileged user accounts must be based upon job function and authorised by the SRO.

3.5. 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. Access to systems by individual users must be authorised by their manager or SRO.

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

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

3.6.2. 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.

3.7. It is the responsibility of the School Business Manager or SRO to ensure that leavers return their devices of their last working day.

4. Network Access Control

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

4.2. 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.

4.3. 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.

4.4. The SRO will ensure that there is sufficient monitoring of the process to ensure that access control is appropriately implemented according to principles detailed in section 3).

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

4.6. Access control requirements are clearly defined, documented and maintained by the systems administrator, who specify the rights of individuals or groups of users and be approved by the SRO.

4.7. Where common operating systems are adopted, predefined user profiles will be maintained to restrict access.

5. Users will only use their account and access in accordance with GST's Data Protection and Acceptable Use Policies.

6. Users will secure their credentials in line with GST's Password Policy.

7. Compliance with this policy will be assessed regularly. Any violation of this policy must be investigated and may result in disciplinary action being taken. In the following exceptional cases compliance with some parts of the policy may be relaxed:
    - If complying with the policy would lead to physical harm or injury to any person.
    - If complying with the policy would cause significant damage to the school's reputation or ability to operate.
    - A request from a law enforcement agency.
    - Medical incapacity or deceased user account access
    - If an emergency arises. In such cases, the user concerned must take the following actions:
        I. Ensure that their manager is aware of the situation and the action to be taken.
        II. Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report.
        III. Ensure that the situation is reported to the office and the Headteacher as soon as possible.

Related Policies

GST Password Policy

GST Acceptable Use Policy

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