Technical Security and Backup Policy

Stroud High School

Contents

PURPOSE 3
1. Technical Security 3
2. Password Security 3
3. Staff/Student Passwords 4
4. Training/Awareness 4
5. Data Backup 5
5.1. Regular data back-up is a requirement for the following: 5
5.2. Backup Logs 5
5.3. Data Stored on Laptops 5
5.4. Data Restore 6
5.5. Backup Hardware and Software 6
5.6. Reviewing the Backup Strategy 6
5.7. Off Site Storage 6
5.8. Testing Data Restoration 6
Appendix 1 7
Appendix 2 - Current Backup Strategy (September 2025) 8

PURPOSE

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Stroud High School (the School) will be responsible for ensuring that the School infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the School's policies)
- access to personal data is securely controlled in line with the School's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of School computer systems
- there is oversight from senior leaders and these have impact on policy and practice

Responsibilities

The management of technical security will be the responsibility of the IT Network Manager.

Terminology

The term 'User' is used to define any person using a device to access the School network. This could be a member of staff, visitor or student.

Responsibilities

The management of technical security will be the responsibility of the IT Network Manager.

1. Technical Security

The School will be responsible for ensuring that the School infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the School meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of School academy technical systems .
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices, etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff.
- All users will have clearly defined access rights School technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager/Technical Staff and will be reviewed, at least annually.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The IT Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- School technical staff regularly monitor and record the activity of users on the School technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by IT staff to control workstations and view users' activity. An agreed protocol is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School system.
- The Personal Information Handling Policy describes the extent of personal use that users and their family members are allowed on School devices that may be used out of School.
- The Personal Information Handling Policy describes the use of removable media (e.g. memory sticks) by users on School devices.
- The School infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans, etc.

2. Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all School technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

- All users will have clearly defined access rights to School technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or another group).
- All School networks and systems will be protected by secure passwords that are regularly changed.
- The "master/administrator" passwords for the School systems, used by the technical staff, must also be available to the Headteacher and Leadership ICT Strategy Lead and kept in a secure place (e.g. School safe). Consideration should also be given to using two-factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users must comply with the complexity protocols identified below.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the staff and student sections below.
- The level of security required may vary for staff and student accounts and the sensitive nature of any data accessed through that account.
- Multi-factor authentication will be enabled for Microsoft 365 and will apply to all staff. Staff will be required to setup an authentication token, either hardware or mobile phone prior to accessing 365.

3. Staff/Student Passwords

- All stake holders will be provided with a username and password by the IT Team who will keep an up-to-date record of users and their usernames.
- The password should be a minimum of 14 characters long and must be made up of 3 random words.
- The account should be "locked out" following five successive incorrect log-on attempts.

- Temporary passwords, e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption).
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of School.
- Passwords should be changed every 365 days.
- The last two passwords cannot be re-used by the same user.
- Passwords should be different for different accounts to ensure that other systems are not put at risk if one is compromised.

4. Training/Awareness

Members of staff will be made aware of the School's password policy:

- at induction
- through the School's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils/students will be made aware of the School's password policy:

- in lessons
- through the Acceptable Use Agreement

Audit/Monitoring/Reporting/Review

The IT Network Manager will ensure that full records are kept of:

- User log-ons
- Security incidents related to this policy

5. Data Backup

Data held on the School's IT network will be backed up to ensure it can be recovered in case of any disaster. The strategies/systems in place must be robust enough to ensure the recovery of data in any circumstance.

5.1. Regular data back-up is a requirement for the following:

- All School data (see Appendix 1 for definition)
- MIS Database
- Email System
- Virtual Servers

5.2. Backup Logs

The IT Network Manager will monitor backup logs to ensure that all data is being backed up correctly.

5.3. Data Stored on Laptops

The School does not backup any data stored on School-owned laptops. All data should be stored on the School's IT network (H:, G: drive, etc.). There are instances where users may want to store data locally on their laptop to work on at home – in these circumstances it is the responsibility of the member of staff to make their own backup of these files. This can simply be achieved by saving these files back to the School network when they are back in School.

5.4. Data Restore

Only the IT Support team have access to restore any data. The IT Network Manager will determine if a restore is possible depending on circumstances.

5.5. Backup Hardware and Software

The IT Network Manager is responsible for the appropriate hardware and software backup systems that are necessary to provide reliable backup and restore facilities. These systems will be reviewed as necessary and should the needs of the School change the IT Network Manager will submit plans to the Leadership Team for new systems.

5.6. Reviewing the Backup Strategy

The IT Network Manager will be responsible for reviewing the backup strategy annually and making any changes that are required.

5.7. Off Site Storage

In the event of a disaster (fire, flooding, etc.) it is good practice to store a copy of data off-site. Our off-site location is the Junior School building and every other monthly tape backup set will be stored off-site.

5.8. Testing Data Restoration

The backup system is only as good as any successful restoration of data. The system should be regularly tested and improvements made if needed.

For Current Backup Strategy see Appendix 2.

Appendix 1

- All School Data (see 5.1 above)
- School
- Staff
- Students
- Year folders
- ICT dept

365 Tenancy:

- Email
- SharePoint
- One-Drive

The IT Network Manager must keep this list updated.

Appendix 2 - Current Backup Strategy (September 2025)

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server (admin and curriculum files)	Synology NAS / Backup Server / External USB Drive	Daily Incremental, Full at Weekends / Weekly (2 sets)
School MIS (SIMS database)	Synology NAS / External USB Drives	Daily Incremental, Full at Weekends / Daily and Weekly
Cloud Services (365)	Synology NAS / Offline Backup	Daily Incremental, Full at Weekends
Email System (365)	Synology NAS / Offline Backup	Daily Incremental, Full at Weekends
All virtual servers / Domain Controller / Hyper V Servers	Synology NAS / Backup Server / External USB Drive	Daily Incremental, Full at Weekends / Weekly (2 sets)

Daily Volume Shadow Copy Backup
This is enabled to cover the period during the School day when a new file could be created and deleted without being backed up in the evening, Volume Shadow Copy makes a backup of these files at various times during the School day.

Every day @ 7.00, 8.30, 10.00, 11.30, 13.00, 14.30, 16.00 and 18.00.

This is for the Main File Server SHS-FS1.

The IT Network Manager must keep the strategy updated.

Date of Policy: October 2020
Reviewed: October 2025
Next Review: October 2026
Monitored by: Resources Committee