Moorpark Junior School

Reach • Believe • Explore • Achieve

Jackfield Infant School

Alexandra Infants

Alexandra Junior School

THE

NEW GUILD

TRUST

Technical Security Policy

POLICY

This policy has been adopted on behalf of all academy schools in the New Guild Trust:

Moorpark Junior School
Jackfield Infant School
Alexandra Junior School
Alexandra Infants' School

Approval and Review

Committee to Approve Policy	Trust Board
Date of Trustee Board / Academy Committee Approval	February 2026
Chair of Trustee Board / Academy committee	Mrs L Eagle
Signature	L Eagle
Accounting Officer	Mrs K Peters
Signature	K Peters
Policy review period	12 months
Date of policy review	February 2027

Version Control

Version	Date Approved	Changes	Reason for Alterations
Initial	Mar 2022	Added Securus Software	New system
	Feb 2023	No change	
	Feb 2024	No change	
	Feb 2025	No Change	
	Feb 2026	Updated with Staffs Tech	

CONTENTS

1. Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure 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.

2. Responsibilities

The management of technical security will be the responsibility of Staffs Tech Ltd (IT Support services).

3. Technical Security Policy Statements

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that the 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 – Staffs Tech Technicians.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the School Secretary/Technical Staff and will be reviewed, at least annually, by the Governors/Trustees.
- Users will be made responsible for the security of their username and password. Users must not allow other users to access systems using their log in details and must immediately report any suspicion or evidence that there has been a breach of security.
- The SBM/School Secretary and IT Technicians are 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.
- Mobile device security and management procedures are in place (please see mobile phone protocol policy).
- 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 (VPN) are used by staff to control workstations and view users' activity.
- An appropriate system is in place for users to report any actual/potential technical incident to Technicians. A work log is created for the Technicians to complete on visits.
- Acceptable Use Policies and Personal Data policies are in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed

on school devices that may be used out of school. This also includes the downloading of executable files and the installation of programs on school devices by users.

- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans, etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

4. 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 Environments (VLE).

Policy Statements

- 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 Governors/Trustees.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The “master/administrator” passwords for the school/academy systems, used by the technical staff must also be available to a member of the SLT 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 will be allocated by Staffs Tech technical support. Any changes carried out must be notified to the manager of the password security policy (above).
- 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 in 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/pupil sections below.
- Requests for password changes should be authenticated (by the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a Line Manager for a request from a member of staff or by a member of staff for a request from a pupil).

Staff Passwords

- All staff users will be provided with a username and password by Staffs Tech Technical support.
- The password should be a minimum of 6 characters long and must include 3 of the following – uppercase character, lowercase character, number, special characters.
- Must not include proper names or any other personal information about the user that might be known by others.
- 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.

Pupil Passwords

- Users will be provided with a username and password by Staffs Tech Technicians, who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children. QR codes will also be used as a log in to sites (where applicable).

Training/Awareness

Members of staff will be made aware of the school’s password policy:

- At induction
- Through the school's online safety policy
- Through the Acceptable Use Agreement.

Pupils / students will be made aware of the school's Security Policy:

- In lessons – Computing/E-safety
- Through the Acceptable Use Agreement.

Audit/Monitoring/Reporting/Review

The responsible person will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy.

5. Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.
Schools also use Securus filtering.

Responsibilities

The responsibility for the management of the school's filtering system will be via Staffs Tech. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering system must:

- be logged in change control logs.
- be reported to a second responsible person: Headteacher/SLT or any person with delegated responsibility.

All users have a responsibility to report immediately to SLT any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is frequently monitored through Securus Software. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff (Staffs Tech Technicians). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- The Acceptable Use Agreement/Policy
- Induction training

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Headteacher/SLT, who will decide whether to make school level changes. The school will not remove filtering systems for the use of social networking.

Monitoring

The school sites website filtering is managed by either local firewall or broadband offsite firewall. This is controlled across the whole site for all members of staff and children.
Forensic software is in place via a company called Securus. This does screen monitoring as well as keystroke monitoring for safeguarding purposes whether that is in google searches or typing in a word document. Forensic monitoring will be completed by SLT or outsourced to a suitable monitoring provider – e.g. Securus Software.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Senior Leaders
- E- safety Governor/Local Community Governing Body committee
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.