
# Security Policy

# (Including Technical Security)

**Stonehill Avenue**
**Birstall**
**Leicester**
**LE4 4JG**

# Contents Page

Our aim is to provide a safe and secure environment for our pupils, staff and visitors. Our Security Policy ensures that we have in place effective procedures to enable us to achieve this aim, including our technical security.

## 1. Roles and responsibilities

### Management Responsibility

School security is shared between the Managing Director, Executive Board, The Head Teacher and the Senior Management Team

### Role of the Managing Director and Executive Board

The Managing Director is responsible for formulating the Security Policy and monitoring its implementation with input from the Executive Board where required.
Any key issues that arise are taken to the full Board and they will assist in key decision making.

### Role of the Head Teacher

The Head Teacher will be responsible for implementing the security policy agreed by the Managing Director.
The HeadTeacher will ensure:

- The staff appreciate the importance of security and understand the school's policy and their responsibilities.
- Staff training needs are kept under review and training as necessary.
- Where necessary, parents are informed of the security policy and encouraged to help.
- Risk assessments are conducted by an appointed person within the school and updated on a regular basis.
- A full school risk assessment should be in place that includes security measures.
- In addition, routine security checks are carried out on an on-going basis by an appointed person. This can form part of regular site walks.
- Timely reports are made to the Managing Director regards any security issues.
- All crimes are reported to the Police.

### Role of the Senior Management Team

- To be aware of the security policy and assist the Head Teacher to ensure that security measures are met
- Ensuring a nominated person is responsible for implementing the school lock up procedure each day. (see point 5)

## 2. Guidelines for school security

### Security of Pupils, Staff and Visitors

### *Security Strategies in School*

### Staff:

- Staff based in school are the only staff to know the combination of any door locks. They should all be equipped with relevant keys and fobs for access arrangements. If any of these are lost or misplaced it must be reported and recorded immediately.
- Staff to contact a member of the Senior Management Team in an emergency.
- Staff to have meetings with parents in designated meeting areas or in the pupils classroom only.
- All staff must challenge visitors who are not wearing a visitor's badge.

## Visitors:

- All visitors, including contractors, to come to main reception entrance, report to School Administration Assistant, sign in the visitors' Registrar System and wear a visitor's badge.
- All parents to make an appointment to meet with a member of staff. To follow the same procedure as above.
- All other services based in the School must sign in at reception
- Parents and visitors to be reminded of our security arrangements via the school Registrar system. The introduction statement on the Registrar system should be reviewed regularly, all visitors and parents must agree to this before entering the building.
- Key changes should be communicated to parents in emails, letters home or newsletter.
- All staff must ensure that the people trying to gain entry to the School should enter via the reception. They should not gain entry through any fire escapes or additional entry points. .

### Hardware:

- A fob system operates on the main entrances to school. A secondary form of security, either a door lock, padlock, or shutter must be used.
- All external doors to be kept closed (doors can be opened internally but not externally).
- All rooms containing equipment that may pose a risk to be kept locked - e.g vocational / practical rooms, I.T. rooms, meeting rooms, science, school kitchen and rooms containing cleaning equipment.
- All upstairs windows to be secured. They do not open fully.

- Only restricted people to have alarm codes or fobs to activate/deactivate alarms

### Outside School:

- School gates / shutters to be kept locked out of school hours.
- School gates (If applicable) to be kept closed and padlocked during school hours.
- Learners must not play in areas marked as out of bounds - by the school gates, sheds, etc.
- All staff to challenge visitors on the school grounds during playtimes, break and lunch.
- Risk assessments must be put in place for activities out of school hours. All security elements must be considered.

## 3. Security of Equipment:

### Inside School Building

- All expensive, portable equipment to be marked as belonging to the School.
- All valuable and recognisable equipment to be on the school asset register .
- Staff to be responsible for returning equipment to secure areas.
- Staff to “sign out” equipment which is taken home, e.g. laptops

### Outside School Building

- Climbable walls and drain pipes connected to the school should be identified and appropriate measure should be put in place to prevent learners from climbing.
- Where appropriate Security fencing, shutters, gates etc should be considered to prevent intrusion.
- Security of Staff, Visitors, Pupils and Equipment during whole-school events should form part of risk assessments.
- The school must provide a form of safe storage for staff personal belongings.
- All portable devices to be stored in rooms that are locked, not left out overnight and in school holidays.
- All rooms to be locked overnight and in school holidays

### Events, e.g. open evenings, parents evenings etc

- All rooms apart from those required to be locked.
- All expensive equipment and personal belongings to be stored safely and securely.

## *Monitoring of strategies*

- Informally through verbal reports from staff and visitors.
- Formally through SMT meetings, regular “Premises, Health and Security” walks
- All staff to take shared responsibility to ensure the security strategies are implemented.

## 4. School Vehicles

- Keys and spare keys for school vehicles to be stored securely in a locked drawer or cupboard when not in use.
- Keys to be stored in a vehicle pack which includes mileage record sheets, contact details for emergencies, fuel cards, breakdown cover
- Driving at work policy to be signed by all staff using vehicles. Relevant documentation must be checked
- All staff to record the mileage and details of each trip
- Vehicle's to be parked securely at school premises, where possible within locked gates at all times.
- If for logistical reasons a school vehicle is kept overnight at a staff members house the insurance company must be made aware and an appropriate check must be made to ensure the school vehicle is in a suitably secure location.
- Staff members are not to use school cars for personal reasons. However, if this is required for the benefit of the school or in the case of an emergency the staff member must sign the form entitled “Additional Use of Company Vehicle” and agree to the terms and conditions.
- All staff members using the company vehicles must have high regard for there security when in use. This includes but is not limited to - not leaving valuable or desirable items on show, parking in secure locations, ensuring the vehicle is locked, taking care and consideration for the keys, etc,

## 5. Lock Up Procedure

The school’s Senior Management Team should ensure that a person is responsible and fully understands the school lock up procedure. If this is completed by a single person they must be fully aware of the schools **Lone Working Policy** (see Employee handbook).
Any person completing the school lock up should have be given clear guidelines by a member of the Senior Management Team
The lock up procedure should be detailed for the school and reviewed regularly. It should include the following as a minimum

- Ensuring all doors are locked
- Ensuring lights are turned off, unless they are used as security lights
- Alarm the building where an alarm system is available
- Ensure all computers have been shut down
- Ensure all high risk appliances have been turned off, e.g cooker, electric heaters, lava lamps, fans, etc

# 5. Technical / Electronic Security

## 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 / 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 and shared files).
- Access to personal data is securely controlled in line with the school's data protection 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 via a year GDPR audit with clear actions and recommendations.
- there is oversight from senior leaders and these have impact on policy and practice.

The school  has a managed ICT service provided by an outside contractor (GGPM and VOIP-4work), it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the *school* itself (as suggested below). It is also important that the managed service provider is fully aware of the *school's*  Online Safety Policy /  Acceptable Use Agreements).

### Responsibilities

The management of technical security will be the responsibility of the Managing Director, Head Teacher and ICT leads/technicians within the school.

### 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 policies and procedures approved within this policy are implemented.  It will also need to ensure that the relevant people 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 (refer to - Local Authority / other relevant body technical / online safety policy and guidance)

- 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, workstations, 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 via GGPM
- 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 GGPM and will be reviewed, at least annually, by GGPM and the schools Managing Director / Data Protection Officer
- Users will be made responsible for the security of their username and password. Under no circumstances should they 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.
- GGPM 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 for school provided devices and / or where mobile devices are allowed access to school systems. Staff may access the school network on personal devices if they are given approval to do so. It is not advised unless necessary to perform work related duties or keep abreast with information sharing. Password protection and automatic sign out for this is in place.
- GGPM 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.
- An appropriate system is in place (direct reporting via email) for users to report any actual / potential technical incident to the Managing Director, ICT lead or ICT Technician.
- An agreed system is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system. This is managed by GGPM
- An agreed policy is in place (e-safety policy) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed process is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Staff training in August/September 2018 in line with new GDPR regulation means the school will seek to eliminate the use of removable media.
- 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.

### 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).

## 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 GGPM and the Managing Director and will be reviewed, at least annually..
- 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 *Managing Director* and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- 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.
- Passwords for new users, and replacement passwords for existing users will be allocated by GGPM, the Managing Director or the ICT Technician.
- Passwords for new users and replacement passwords for existing users will be issued through an an email system via GGPM
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below.

### Staff passwords:

- All staff users will be provided with a username and password by GGPM
- The password should be a minimum of 8 characters long and must meet Google requirements
- Must not include proper names or any other personal information about the user that might be known by others
- The account should be “locked out” following 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)

- Should be changed at least every 60 to 90 days (student passwords will not be changes due to SEN needs)
- Should not be re-used for 6 months and be significantly different from previous passwords created by the same user. The last four passwords cannot be reused.

### Student / pupil passwords

- All users will be provided with a username and password by GGPM who will keep an up to date record of users and their usernames. Primary learners and those with SEN would may not remember usernames and passwords will need to share this information with their key worker / class tutor
- *Users will **not** be required to change their password due to SEN*
- Students / pupils will be taught the importance of password security as part of their ICT curriculum.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

### Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users:
Members of staff will be made aware of the school's password policy:

- At induction
- Through the school's online 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
- At Induction
- Through the Acceptable Use Agreement

### Audit / Monitoring / Reporting / Review

The responsible person (GGPM) will ensure that full records (manual or automated) are kept of:

· User Ids and requests for password changes
· *User log-ins*
· *Security incidents related to this policy*

## 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.

### Responsibilities

The responsibility for the management of the school's filtering will be held by GGPM. 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 service must:

- Be logged in change control logs
- Be reported, discussed and agreed with the Managing Director:

All users have a responsibility to report immediately to GGPM, the Managing Director, the ICT Technician or ICT Leads 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 programmes 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 logged and frequently monitored. 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.

- The school manages its own filtering service via GGPM
- The school has provided enhanced / differentiated user-level filtering through the use of the Google Education filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)
- 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 Managing Director
- Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems
- 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 Head Teachers and the Managing Director. If the request is agreed, this action will be recorded and logged.

### Education / Training / Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme delivered in ICT lessons. 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
· Induction training
· Staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement they sign for their child and through online safety awareness sessions / newsletter etc.

### The Filtering System

In this section the school should provide a detailed explanation of:

- Requests to change or remove filters should go to the Head Teacher or Managing Director via email
- The person requesting will be notified of the decision. There should be a strong educational reason for the request
- GGPM will provide their advice on the changes and will log the request and change.

.

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 any member of the Senior Management Team who will refer to the Head Teacher or Managing Director to decide whether to make school level changes (as above).

## Monitoring

ALP Schools operates with Google Education monitoring systems
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement.

## Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the Managing Director, Head Teacher and the Executive Board on request
This policy may be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.