Xavier Catholic Education Trust
Security Policy

This policy has been approved and adopted by the Xavier Catholic Education Trust in Oct 2022 and will be reviewed in Oct 2024.

Committee Responsible: Audit and Risk Committee

Contents

1. Introduction

Xavier Catholic Education Trust recognises and accepts its corporate responsibility to provide a safe and secure environment for children, employees and visitors to all of its schools and to ensure that we take appropriate measures to protect our physical and IT based assets.

Each school's security procedures will operate within the framework described in this policy with additional reference to the Xavier Child Protection and Safeguarding policies, the Xavier Health and Safety policy and the Xavier Emergency Management Business Continuity plan. Where appropriate the Trust will seek any necessary expert advice to determine the security risks and precautions required to deal with them.

Xavier Catholic Education Trust will provide staff with enough resources, information and training to implement the security procedures. The Trust must be informed of breaches andfailures of the policy, to enable them to take any corrective action necessary to ensure the safety of children and staff.

2. Organisational Responsibilities

The following groups and/or individuals have responsibilities for ensuring the security of each school.

Xavier Catholic Education Trust

Xavier Catholic Education Trust will:

- ensure that each school is aware of the security policy and that this has been implemented successfully;
- monitor the performance of the schools security measures;
- delegate the day to day implementation of the policy to the Headteacher / Head of School;
- review the policy every two years.

The Headteacher (also incorporating the post of Head of School)

The Headteacher will:

- ensure arrangements within the school comply with the security policy;
- ensure that all staff within the school receive information, instruction and training in the security policy and its procedures;
- establish a system for reporting, recording and investigating breaches of

the policy and take reasonable steps to prevent reoccurrence.
- ensure that all visitors, contractors and agency staff adhere to the security policy;
- monitor the implementation of the policy and security arrangements.

Staff members

All staff members will:

- comply with this policy and the arrangements made by the Headteacher to ensure the safety of children, employees and others on site;
- report immediately any breaches of the security policy to the Headteacher.

Pupils

All pupils will:

- be encouraged to exercise personal responsibility for the security of themselves and others;
- co-operate with the arrangements made for the security of the school.

3. Physical Security Arrangements

Each school must have adequate arrangements to ensure the safety and security of staff, pupils and other persons using the school premises.

3.1 Information and Communication

- All staff must be aware of the school's security procedures, especially staff that have been given a specific role to play.
- All staff inductions will include an overview of their role within school security.
- Security arrangements must be communicated to all third parties that use the premises and grounds. All site users will be expected to comply with the security arrangements as a condition of accessing the site.
- Parents must be informed about the security arrangements and any part they are expected to play, for example, when visiting the school or at handover

3.2 Controlled access and egress during the school day

Controlled access is a combination of measures to ensure that unauthorised visitors do not present a risk to pupils or staff.
The extent of physical controls, such as fences, must be decided by a robust risk assessment of the physical environment, measured against the likelihood of visitors presenting a risk and the reasonableness of the control measures needed to reduce this risk.

Access Control
Each school must take all reasonable efforts to restrict access to the buildings and prevent unauthorised access to children and staff.

Security of the Building
- Security lights must be on whilst the premises are occupied after dark.
- Class teachers are to make sure that their classroom is secure, windows closed and equipment switched off before leaving the premises.
- External doors must not be left open/unlocked.
- The site manager must ensure external gates are secured at the agreed times.
- The last key holder to leave the premises is responsible for securing the building if they leave after the premises team.

Alarm Call-Outs
If a key holder is contacted as a result of an alarm activation, they must wait a safe distance away from the school until the emergency support arrives. If necessary, a member of SLT should be contacted for support.

External areas
All external areas within each school, are to be secured by means of physical restrictions such as fencing and padlocked gates

3.3 Early Years External Areas

As pupils require access to the outside areas at all times, each school must ensure that a secure outside area has been provided that has a suitable perimeter fence. This requires fixings that prevent pupils from opening gates and exiting the area without adult supervision.

3.4 People Management

Xavier Catholic Education Trust acknowledges its duty of care to ensure the safety of all our pupils. Critical to this, is the monitoring and control of all adults who come into contact with pupils in line with our safeguarding protocols. To ensure the safety of all pupils the following must take place in each school:

- all staff must be fully vetted before joining each school, including the taking up of references and checks with the Disclosure and Barring Service (DBS);
- a single central register of visitors to each site must be maintained by the Admin Staff/ Headteacher;
- all regular volunteers, visitors and contractors must have DBS checks before working unsupervised with pupils, or moving unaccompanied around the school;

3.5 Control of Visitors

The control of visitors is a fundamental part of Xavier Catholic Education Trust's security policy. This ensures the safeguarding of both people and property. Visitors to the school must wear identification badges to enable the identification of unauthorised visitors by staff and pupils.

3.6 Supervision of pupils

Handover
Handover arrangements (including wrap around care) for the arrival and departure of pupils at each school are communicated clearly to parents and carers on joining the school.

Supervision during breaks and lunchtime
During the school day, all pupils are to be supervised by teachers or support staff when using the playground.

- Parents must give permission in writing, or verbally if they can be recognised and verified as legitimate, for any other person to collect their child from any of our schools.
- No pupil is allowed to leave school during the day for an appointment unless a known adult arrives to collect them from the School Office or written permission is received by the school. The departure and return of pupils must always be logged by the Admin Team.

Taxis
Schools will only use taxi companies where all drivers have been DBS checked.

3.7 Cooperation with third parties, extended services and community groups

Xavier Catholic Education Trust's security arrangements have taken into account

any other third parties that use the school's buildings or grounds. In most circumstances, the arrangements for the school will be equally applicable for the third parties. Additional security measures that apply to the groups listed, are given below.

- All After School Clubs - are to be managed and supervised by existing school staff who have enhanced DBS checks.
- Community use - community groups must sign a Letting Form that states that they have appropriate public liability insurance, child protection, first aid arrangements in place and have received information regarding health and safety, security and emergency procedures.

3.8 Supervision of contractors

Contractors and maintenance personnel may not always have DBS clearance. However, if they have not been DBS checked, they must not have unsupervised access to children and must therefore be escorted on school grounds at all times.

If the school has been advised by his/her employer, that the contractor has a clear, current DBS check, and has received notification, in writing on headed paper, of the DBS reference number and date of check, they will be able to move around on site unaccompanied.

3.9 Lone Workers

Please see the Xavier Health and Safety policy

3.10 Physical security measures

Xavier Catholic Education Trust has considered the need to use physical measures such as fencing and electronic access controls to ensure the safety of staff and pupils. Each school must review the provision of physical security measures on a regular basis in the form of a security risk assessment.
The risk assessment must take into account:

- the location and layout of the school;
- past incidents related to security;
- the performance of other security measures already in place or that could be implemented;
- the cost of physical security improvements and the availability of funding.

Where justified, by the consideration of the risk, each school must ensure that physical security measures are installed. Where physical controls are not justified, each school must ensure that other controls are implemented to ensure the safety

of staff and pupils.
Where electronic controls are installed, for example alarm systems, they must be maintained as recommended by the manufacturer.

3.11 Trespass and Nuisance

In the first instance, members of the Senior Leadership Team within each school, should consider the level of risk and may approach an unauthorised member of the public. If pupils are outside, it might be necessary to take pupils back to their classrooms. However, in any case where such measures fail to resolve the situation, recourse to the law will be considered. This extends to unlawful presence on site, individuals creating a nuisance or disturbance, verbal abuse of pupils or staff, as well as violence to any individual. Any such situation will be contained as appropriate at the time, but as this is a criminal offence the school should always refer to the police.

3.12 Serious Incidents or Threats – please refer to the Xavier Emergency Management and Business Continuity Plan.

In the event of any serious incident, staff should:

1. Stay calm.
2. Minimise the risk to themselves, the pupils and others.
3. Seek help as soon as possible.

- The welfare, security and protection of the pupils, staff and visitors will take precedence over any other action required to contain the situation.
- The Headteacher / Head of School or other senior members of staff must be informed. This person will then decide what action to take, which may involve contacting parents or the police.
- After any such event, a detailed report must be prepared by a nominated individual, for presentation to the Trust. If required, an emergency meeting will be held by Xavier Catholic Education Trust to review, make recommendations and take appropriate action.
- Statutory bodies, such as the Police, Local Authority, etc., will be informed and consulted as required. All schools should seek to follow best practice guidelines in its response and handling of threats and incidents.

3.13 Theft and Burglary

Schools are not immune from burglary or from theft of belongings, monies and the personal items of pupils. Each school must take an active stance on this, with items of high value added to the school inventory and the speedy banking of all monies, so that large sums are not left on the premises.

Valuables left on any Xavier premises should be stored in a locked cabinet. Suitable locks must also be used on doors and windows. Each school must actively encourage personal security awareness. Pupils and staff must be discouraged from bringing items of value to school.

Any incident of theft will be investigated. Xavier Catholic Education Trust will not accept liability for the loss of personal belongings.

3.14 Locking arrangements

At various times throughout the day, security arrangements are required such as the locking of various entrances and exits.
Locking arrangements for each school are controlled by the Headteacher as necessary.

3.15 CCTV

Our schools make use of CCTV systems as part of their security procedures. These systems have the ability to record incidents to enable evidence to be presented to the appropriate authorities. Each school must ensure:

- adequate signage is present;
- data protection regulations are followed;
- members of the public cannot see any images being recorded;
- a log is kept of times the footage has been accessed.

3.16 Cash Handling

All schools are expected to avoid keeping cash on the premises wherever possible. Safes must be used and kept locked at all times. Staff must avoid handling cash in visible areas. Any money requiring banking should be taken at irregular times, particularly where substantial sums are involved.
More details are provided in the Financial Procedures Manual.

3.17 Items of Value

All items above the value of £150 (or desirable items) must be recorded in the schools asset register. Items of value, such as portable equipment with a value above £250, must not be left unattended in rooms where there is public access. In such locations, the room must be locked when it is vacated.
Wherever possible valuable items must not be left where visible from outside. The security risk assessment must take into account the location and security arrangements for high value equipment, for example ICT equipment.

3.18 Security of Equipment

All items of equipment within each school, are the property of the school and as such must be kept well maintained and secure at all times. Staff may be permitted to take some mobile equipment out of the building, but they must seek authorisation from an appropriate member of the leadership team.

3.19 Personal Property

Personal property will remain the responsibility of its owner. This includes staff, pupils and visitors. All building users should be discouraged from bringing to school any valuable personal property.
Lost property should be handed to the School Office, where it will be kept for 6 months before disposal.

3.20 Medicines

There are on occasion when pupils may be prescribed medicines which must be taken during school time. Parents will provide such medicines in suitable and labelled containers. These containers will be locked in the school's medicine cabinet.
Arrangements for the administration of medicines are detailed in the Xavier First Aid policy.

IHCP (Individual Health Care Plans) should be completed when a child takes medicine at school or has a medical condition that the school should be aware of; such as allergies, the use of EpiPens etc.

3.22 Curriculum Activities

Pupils should be made aware of security issues according to the level of their understanding. Where appropriate, they must be:

- encouraged to be security conscious e.g. never open external doors to adults other than known staff;
- discouraged from approaching any adult who they do not know and to tell a safe adult;
- taught how to take care of themselves and others.

Schools are encouraged to take advantage of any opportunity to heighten pupils' awareness of security issues. Pupils should be listened to and their fears and concerns respected.

4. IT Security Arrangements

4.1 Data Security

The General Data Protection Regulation (GDPR) requires organisations to put in place appropriate technical and organisational principles and safeguard individual rights. This means that we have to integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle. Schools must ensure that privacy and data protection is a key consideration in everything they do. As part of this they must:

- Consider data protection issues as part of the design and implementation of systems, services, products and practices.
- Make data protection an essential component of the core functionality of their processing systems and services
- Anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals

Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities. Having a data sharing agreement in place helps demonstrate you are meeting your accountability obligations under the GDPR.

4.2 Data Access Control

Staff should only access systems for which they are authorised.

Access privileges will be modified/removed as appropriate when an individual changes job or leaves. Managers must ensure they advise IT Support of any changes requiring such modification/removal. System administrators will disable all accounts relating to members of staff who leave the employment of the trust on their last working day. The employee's manager should ensure that all files of continuing interest to the trust or school are transferred to another user before the member of staff leaves.

Managers must ensure that staff leaving the trust's employment do not inappropriately wipe or delete information. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to trust information and equipment.

4.3 Security and Storage of Information

All information, whether electronic or manual, must be stored in a secure manner appropriate to its sensitivity. It is for each school to determine the sensitivity of the information held and the relevant storage appropriate to that information.

Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- At no time should sensitive, confidential or personal information be stored on a portable hard drive unless encrypted.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

4.4 Emailing Information

If information is particularly sensitive or confidential, the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information. It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

Sending information by email:

- Carefully check the recipient's email address before pressing send - this is particularly important where the 'to' field autocompletes
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list.
- Take care when replying 'to all' - do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password e.g., telephone call or text
- Consider the use of secure email where this is available or encrypt the document

4.5 Security of IT Equipment

Portable computers must have appropriate access protection, for example, passwords and encryption, and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times. The equipment should only be used by the individual to which it is issued.

Staff working from home must ensure appropriate security is in place to protect trust equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring trust equipment and information is kept out of sight.

Staff who use portable computers belonging to the trust must use them solely for business purposes. Trust issued equipment must not be used by non-trust staff.

4.6 IT Cloud Storage

All Xavier staff have been provided with a trust/school cloud account for the sharing and storage of files. Staff should not use personal cloud storage solutions for the transfer of trust/school information.

4.7 Physical Access to Servers

All servers and associated network equipment should be in secure areas and where appropriate within locked cabinets. Unrestricted access to the servers/network equipment will be confined to designated staff whose job function requires access to that equipment.

4.8 Use of Removable Media

The use of removable media such as USB sticks, thumb drives etc. should be avoided. If there is a valid business case for removable media, then the device must be encrypted.

4.9 Data Backups

All data should be held on a network directory or authorised cloud storage platform; this will ensure routine backup processes capture the data. Information must not be held locally on a PC hard drive as this will be lost in the event of a hard drive failure. Data should be protected by clearly defined and controlled backup procedures which will generate data for archiving and recovery purposes.

System administrators should produce written backup plans for each system under their management. Where removable media (tape, caddy etc.) is used, the media should be clearly labelled and held in a secure area. The 3-2-1 approach to data backup should be carried out, whereby 3 copies of the data are kept on 2 different types of media and 1 copy is kept in a remote location. Several generations of backup should be kept. To ensure that the back-up data is sufficient and accurate, it should be regularly tested.

Archived and recovery data should be accorded the same security as live data and should be held separately. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes.

4.10 Equipment, Media and Data Disposal

Disposal of equipment, media and data must be arranged through IT Support who will arrange for disks to be wiped or destroyed to the appropriate standards.

4.11 Cyber Security Training

Xavier seeks to minimise the risks of computer viruses through education and good practice/procedures as well as anti-virus software.

It is a requirement that all staff and governors who have access to school systems carry out cyber security training provided by the National Cyber Security Centre.

4.12 Antivirus Software

Getting infected with malware - often ransomware - is one of the most common ways that IT systems can be compromised. Malware infection can result in theft of intellectual property, ransoming of data, and/or disruption to services provided by the trust. As such, it's important for organisations to try and prevent malware from infecting their devices and data.

Using antivirus (AV) software is one way of helping prevent infection and should therefore be installed on all Windows PCs and Servers. AV works in conjunction with network defences, device configuration and App Store scanning to try and block malware before it can cause harm to your organisation.

The risk of becoming infected by malware on iOS, Android and Chrome OS devices is minimal, however these devices should be kept up to date with the latest security updates from the device manufacturer. An allow list of permitted third-party applications should be used and restrictions in place through a Mobile Device Management (MDM) platform to prevent the unauthorised installation of applications.

The security built in to macOS is reasonably effective at preventing malware on the platform, but some schools may still wish to install a third-party product.

4.13 Vulnerability Management and Patching

Exploitation of known vulnerabilities in software remains the greatest cause of security incidents. Patching - the process of applying updates from software developers, hardware suppliers and vendors, to either enhance functionality or to improve security is one of the most important things you can do to mitigate vulnerabilities. A regular assessment regime is essential to ensure that your organisation is aware of the risks that are present.

4.14 Vulnerability Scanning

Schools should perform vulnerability assessment of their entire estate regularly. New vulnerabilities are reported all the time and many software vendors release updates on a monthly cycle. A regular assessment regime is essential to ensure that your organisation is aware of the risks that are present.

Software patch status can be collected using software asset management suites, however you should use an automated vulnerability assessment system (VAS) to identify vulnerabilities across your school's IT estate. This process is also known as penetration testing. Xavier carries out this testing on behalf of schools who opt into the central IT service.

4.15 Passwords

Using complexity requirements (that is, where users can only use passwords that are suitably complex) is a poor defence against guessing attacks. It places an extra burden on users, many of whom will use predictable patterns (such as replacing the letter 'o' with a zero) to meet the required 'complexity' criteria. Attackers are familiar with these strategies and use this knowledge to optimise their attacks. Additionally, complexity requirements provide no defence against common attack types such as social engineering or insecure storage of passwords.
For the above reasons it is not recommend to enforce the use of complexity requirements when implementing user generated passwords.

The use of technical controls such as multi-factor authentication and account lock out rules to defend against automated guessing attacks is far more effective than relying on users to generate (and remember) complex passwords. However, you should specify a minimum password length, to prevent very short passwords from being used. Password length should only be capped by the capabilities of your system. Be aware that enforcing excessively long passwords will introduce other burdens (such as time taken to enter passwords, and the increased likelihood of mistyping especially on touch screen devices). Adopting 'the three random words' technique can help users to use suitably complex passphrases that they can actually remember.

4.16 Multi-Factor Authentication (MFA)

One of the most effective ways of providing additional protection to a password protected account is to use MFA. Accounts that have been set up to use MFA require a second factor, which is something that you (and only you) can access. This could be a code that's sent to you by text message, or that's created by an app, so even if an attacker discovers a password, they won't be able to access the associated account without also compromising the other factor.
MFA should be used where there may be additional risk, such as logging into an account on a cloud-based system such as Microsoft 365, Google Workspace or Arbor.

4.17 Single Sign-On

Single sign-on (SSO) allows staff to use just one set of credentials to automatically gain access to multiple applications and services. This massively reduces the pressure on a user to create and remember many passwords. However, if an attacker compromises a user's account or password, that attacker could have easy access to far more content than they might have in a traditional system. For this reason, SSO should be implemented with MFA where possible.

4.18 Timeout Procedures

Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. The time-out delay should reflect the security risks of the area.
Staff must 'lock' their computers, if leaving them unattended for any length of time.

5. Monitoring and Review

The Headteacher must monitor the performance of this policy and report breaches, failings or security related incidents to Xavier Catholic Education Trust.
This policy will be reviewed every two years by the Trust