# LORETO GRAMMAR SCHOOL
# OMAGH

# Cyber Security Policy

***'Striving for Excellence – the* LORETO *way'***

Included: February 2024
Updated: November 2026

**Section 7 Part 20**

# Loreto Grammar School Omagh
# Cyber Security Policy

## 1. Rationale

The purpose of this policy is to set out guidelines to protect the data and technology infrastructure of Loreto Grammar School. As schools become more and more technology-dependant, the greater the risk of a serious security breach of sensitive data and systems. A serious violation could potentially disable the day-to-day functions of the school for an unknown period. This policy applies collectively to staff, pupils, Governors, contractors, and other users who may have temporary or permanent access to school systems and hardware.

## 2. Risks

**What is at risk?**

From a school perspective there is information on IT systems that could be categorised as sensitive and should not be circulated in the public domain. Some examples would be:

1. Financial data.
2. Contact details of staff and pupils.
3. Safeguarding/welfare data for pupils.
4. Governance data.
5. Payroll information.

**Where do potential threats come from?**

- Cybercrime - online organised criminal gangs working towards a financial gain by stealing data and selling it on or by locking organisations out of their systems until a ransom is paid.
- Insiders - a public release of sensitive information by an individual from within an organisation. This can be deliberately released or, as is often the case, in error.
- Hacktivists - Politically motivated groups who take over systems as a means of publicising a cause.
- Physical Threats - flood, fire, power cuts can have a severe impact on the daily operations of a school IT system.
- Zero-day threat - A cyber-attack launched on the same day that a weakness in a software package has been discovered with a view to exploiting the frailty before a fix can be issued.

## 3. Protection

Protection against potential cybersecurity issues will be divided into organisational security and user security. Organisational security will be measures applied globally across the full network infrastructure. User security will be specific actions that individuals apply as part of a routine of good practice and awareness of potential dangers.

### A. Organisational Security

The school (via the EA) has an official relationship with C2K (EdIS and Capita) which is contractually obligated to provide and maintain some of the Cyber Security defence measures. Some of the measures employed to strengthen cyber security are:

- Protected networks with correctly configured firewalls.
- Network devices with security features enabled.
- User accounts which only provide the level of access required for the user's specific role.
- Sensitive information should be secured (where possible) in private folders only accessible by authorised personnel.
- Anti-malware software is in place to protect networks.
- Applications installed on the network are security checked before installation.
- Online devices use properly licensed software and are patched with latest security updates.
- Important data has multiple backups with at least one stored off-site.
- Serious cyber-attacks should be reported to relevant authorities.
- Disseminate good practice to end users.

Any reaction to a cyber security incident will be co-ordinated with the relevant personnel within the Edis/C2K/Capita teams.

**Acceptable Use Policy (AUP) in place at school must:**

1. Be signed by staff (sent via email by Vice-Principal every academic year and printed, signed and returned to Vice-Principal by all staff. Appendix 1).
2. Be signed by students (summary of policies on school website and hardcopy of signatures collected by Form Teacher every academic year).
3. State monitoring is in place, and account or mailbox can be accessed during a security investigation.

**In the event of a potential cyber security incident, the school's ICT & Internet Policy; Cyber Security and/ or Digital Devices and Mobile Phone Policy will be implemented, as necessary.**

### B. User Security

End users can take effective actions to maintain both organisational and personal security by being aware of the following actions to minimise threats:

- Be careful when clicking on links or attachments in emails, even if appearing to be from a trusted source. Do not click on any links in emails from unknown senders, and know the signs of phishing emails. Double clicking on an email address will help identify if it is a trusted email address.
- Never share passwords with others. Use different passwords for different accounts.
- Use strong passwords: a strong password is one that is at least 11 characters long and contains a diverse use of characters (upper and lower case), numbers and symbols.
- Store work allocated devices securely, out of sight and never in a car. Make sure devices are locked with a password if left unattended during a work break.
- When working remotely, be sure to use a password protected wireless network and avoid public networks where internet or cloud-based information could be intercepted by attackers.
- Be mindful of where confidential documents and private information are stored - be sure to only save sensitive documents in the approved locations, and be aware of procedures for physically or electronically sharing this information with others.
- If there is a need to use USB storage, ensure it is encrypted. Never leave USB storage devices plugged in when a device is unattended.
- Always err on the side of caution. If an email looks suspicious, a policy is unclear, or it seems that a procedure isn't being followed, bring it to the attention of the IT Support Team.

## 4. Identifying a cyber security incident

The first step in dealing with an incident is identifying the specifics of what is occurring. Some things that may point to a cyber security incident are:

- Computers running slowly.
- Multiple users being locked out of their accounts.
- Multiple users being unable to access documents.
- Messages demanding a ransom for the release of files.
- People informing you of strange emails coming out of your domain.
- Redirected internet searches.

- Requests for unauthorised payments.
- Unusual account activity.

The following questions will be used to document what has occurred. This information will provide essential information for technical support teams and will also be useful for incident reviews.

- What problem has been reported, and by who?
- What services, programs and/or hardware aren't working?
- Are there any signs that data has been lost? For example, have there been ransom requests, or has data been posted on the internet?
- What information (if any) has been disclosed to unauthorised parties, deleted or corrupted?
- Have users noticed any problems? Can they use services?
- Who designed the affected system, and who maintains it? Relevant to third party contracted services.
- When did the problem occur or first come to attention?
- What is the scope of the problem, what areas of the organisation are affected?
- Have there been any signs as to whether the problem has occurred internally within the organisation or externally through a supply chain?
- What is the potential educational impact of the incident?

## 5. Actions in the event of a potential cybersecurity incident

- The first point of contact when an incident is suspected should be the IT Manager or another member of the IT Support Team. Failing that please contact the C2K Helpdesk on 08000 931541. The IT Support Team will carry out checks to ascertain the nature of the issue. Should initial investigations point to a cybersecurity incident then C2K/Capita/Edis will be contacted for additional investigation.
- If initial investigations point to a cybersecurity incident, this will be escalated to the Principal (or in his/her stead one of the Vice-Principals) to assess if additional action is required.
- If required the school will seek the guidance of Edis/C2K/Capita. (See also https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools).
- If necessary the school Critical Incident Policy will be implemented.

## 6. Review

In the event of a cyber security incident the school will carry out a post event analysis seeking input from all stakeholders and update all relevant policies and practices as a consequence.

- This policy will be kept under constant review by the school's Curriculum Committee who will advise the Board of Governors.
- This Policy will be reviewed annually by the Board of Governors and amended and updated as appropriate. In the course of a review the Board of Governors will:
    - Take account of the findings of any inspection of the school.
    - Take account of priorities expressed in the School Development Plan.
    - Consider the views of staff expressed through subject leaders and of pupils whose views will be expressed through the Student Council.
    - Take account of the views of parents reaching the school through surveying of a random selection of parents.
    - Consider changes required by new statutory requirements.

**Appendix 1:**

**E Safety Acceptable User Policy For Staff and Visitors**

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and any visitors are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs M Gavin, Vice Principal, Loreto Grammar School.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number / social media and personal e-mail address, to pupils.
- I will only use the approved, secure C2K e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of Mrs M Gavin.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Vice Principal / Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- Monitoring is in place and in the event of a data breach, my account or mailbox can be accessed during a security investigation.

**User Signature**

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout Loreto Grammar School.

Signature …….…….…… Date ……

Full Name …….....(printed)

Job title . . . . . .