Marjory Kinnon School

Cyber Security Policy

October 2025

Cyber security has been identified as a risk for the school and every employee needs to contribute to ensure data security.

The school has invested in technical cyber security measures, but we also need our employees to be vigilant and to act to protect the IT systems.

The IT Manager is responsible for cyber security within Marjory Kinnon School.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our Data Protection Policy, Data Breach Policy, Guidance for Acceptable Use of Internet & Technologies and Social Media Policy.

1. Purpose & Scope

The purpose of this document is to establish systems and controls to protect the school from cyber criminals and associated cyber security risks, as well as to set out an action plan should the school fall victim to cyber-crime.

This policy is relevant to all staff and governors.

2. What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.
- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements of our school. The risk to confidential information and personal data is the biggest of all threats from cyber-crime.

- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).
- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.
- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Cyber Response Plan. The Headteacher is responsible for making that decision and communicating with IT.
- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

3. Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the school to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The IT Manager can provide further details of other aspects of the school risk assessment process upon request.

The school has put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

3.1 Technology Solutions

The school has implemented the following technical measures to protect against cyber-crime:

- Firewalls – Maintained and updated by LGFL.
- Anti-virus software – Sophos Intercept x provided by LGFL and installed on all windows and MAC endpoint devices including servers, also features anti-ransomware capabilities.
- Anti-spam software – provided as part of our 365-email exchange tenancy.

- Auto or real-time updates on our OS and applications where possible – Windows updates run automatically on endpoints every week, server updates happen during term breaks.
- URL filtering – provided by LGFL School Protect and updated by the IT team. Includes all lists recommended in KCSIE documentation.
- Secure data backup – Daily incremental offsite file backups provided by LGFL, local backups to storage devices not connected to the network including server VMs and service database backups.
- Encryption – all windows laptops provided have bitlocker disk encryption enabled, the ability to send encrypted emails through 365.
- Deleting or disabling unused/unnecessary user accounts – accounts are disabled as and when directed by the HR Department.
- Deleting or disabling unused/unnecessary software – software is removed from the image if no longer required.
- Using strong passwords – complex passwords are enforced and required to be changed regularly.
- Disabling auto-run features – auto run requires admin credentials.
- Anti-malware software – Malwarebytes provided by LGFL is installed on all windows and mac OS endpoints.
- USB devices disabled – blocked automatically by Sophos when connected to a school device.
- Shared network drives are locked down, so staff only see what they are required to see for their job.
- VPN connection from home – access to school network requires VPN to be connected which is provided by LGFL.

3.2 Controls & Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- Technology solutions in isolation cannot protect us adequately, so our systems and controls extend to cover the human element of cyber-crime/cyber security risk.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the school or any third parties with whom we share data.

- It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be partly achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:
    - Physically ringfencing the individuals or teams working on a matter.
    - Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information.
    - Getting a signed confidentiality agreement from each staff member.
    - Disposing of confidential documents securely.
    - Having a clear desk policy.
    - Discouraging staff from reading confidential papers or discussing sensitive matters in public.

Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.

All staff must:

- Ensure you are familiar with the risks presented by cyber-crime and cyber security attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g. not forwarding chain letters or inappropriate/spam emails to others. We will help you by continually raising awareness of those risks and providing training where necessary.
- Report any concerns you may have.

3.3 Passwords

- Choose strong passwords (the school's IT team advises that a strong password contains
    - Password minimum length at least eight characters.
    - Must include numbers (0-9).
    - Include uppercase letters (A-Z).
    - Include lowercase letters (a-z).
    - Must include symbols/special characters (!,@,#,$,%,<,^,&,* etc.).
- Keep passwords secret.
- Never reuse a password.
- Never allow any other person to access the school's systems using your login details.

- Do not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT Team have installed on their computer, phone or network or the school IT systems.
- Report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the IT Team as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy.
- Only access work systems using computers or phones that the school owns. Staff may only connect personal devices to the guest Wi-Fi provided.
- Do not install software onto your school computer or phone. All software requests should be made to the IT team.
- Avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using school equipment and/or networks.

The school considers the following actions to be a misuse of its IT systems or resources:

- Any malicious or illegal action carried out against the school or using the school's systems.
- Accessing inappropriate, adult or illegal content within school premises or using school equipment.
- Excessive personal use of school's IT systems during working hours.
- Removing data or equipment from school premises or systems without permission, or in circumstances prohibited by this policy.
- Using school equipment in a way prohibited by this policy.
- Circumventing technical cyber security measures implemented by the school's IT team.
- Failing to report a mistake or cyber security breach.

4. Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

- Containment and recovery: To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our Cyber Response plan.
- Assessment of the ongoing risk: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity

of the data should also be confirmed and any consequences of the breach/attack identified.

- Notification: To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
- Evaluation and response: To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, the school will invoke their Data Breach Policy rather than follow up the process above.