LYCÉE FRANÇAIS CHARLES DE GAULLE DE LONDRES
CYBERSECURITY POLICY

Date of Review: February 2024, November 2025
Next Review: October 2026

This policy is publicly available on the School website and is available in hard copy on request.

This is the Cybersecurity Policy of Lycée Français Charles de Gaulle de Londres (the "School").

This policy has been drafted, using the Cybersecurity Policy template published by LGfL (a charitable trust whose mission is the advancement of Education) as a starting point.

Mission statement

The School makes a simple and honest commitment: to offer each child the best conditions in which to realise their academic potential, to be able to develop and thrive in a peaceful environment and achieve the level of excellence required to access their desired course even at the most competitive universities. We nurture each individual with care and help them build self-confidence – this remains our pledge to our families as much today as it has been for over a century.

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.
This Cybersecurity Policy outlines the School 's guidelines and security provisions which are there to protect the School's systems, services and data in the event of a cyberattack.

1. Scope of Policy

This policy applies to all Lycée Français Charles de Gaulle staff, contractors, volunteers, pupils (in relation to Section 12) and anyone else granted permanent or temporary access to the School's systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the School.

2. Risk Management

The School will include cybersecurity risks on its organisational risk register, ATLAS, regularly reporting on the progress and management of these risks to Proviseure and the proprietor's representative.

3. Physical Security

The School will ensure there are appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

4. Asset Management

To ensure that security controls to protect the data and systems are applied effectively, the School will maintain a register of personal data processing operations listing files/systems that hold personally identifiable data and special category data, and asset registers for all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

5. User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform IT Support as soon as possible. Personal accounts should not be used for work purposes. The School will implement multi-factor authentication where it is practicable to do so.

6. Devices

To ensure the security of all the School issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to IT Support (support@lyceefrancais.org.uk)
- Change all account passwords at once when a device is lost or stolen (and report immediately to IT Support (support@lyceefrancais.org.uk)
- Report a suspected threat or security weakness in the School 's systems to the IT Manager

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

7. Data Security

The School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

The School defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information

Critical data and systems on the School's main site will be backed up on a regular basis following the 3-2-1 backup methodology

- 3 versions of data
- 2 different types of media
- 1 copy offline

8. Sharing Files

Lycee Francais Charles de Gaulle recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping the School 's files on the School systems
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting IT Support (support@lyceefrancais.org.uk) and the School's Data Protection Officer (dpo@lyceefrancais.org.uk) to any breaches, malicious activity or suspected scams.

9. Training

The School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

10. System Security

The School's IT Manager, with the assistance of the IT support team will build security principles into the design of IT services for the School:

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software
- before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

11. Major Incident Response Plan

The School will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers (involving the direction, the IT manager, the Health and Safety manager, the Premises manager and the proprietor's representative)
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

12. Cyber security of public examinations governed by the JCQ and Cambridge

The School is committed to ensuring the integrity and security of examinations conducted under the Joint Council for Qualifications ("JCQ") framework and Cambridge International Education ("Cambridge") regulations. In light of the increasing threat of cyber attacks, the School, also referred to in this Section 12 as "the Centre", has formulated this policy to safeguard the examination process and maintain the fairness and integrity of assessments.

The Centre is dedicated to maintaining the highest standards of security in examinations. This policy reflects the Centre's commitment to safeguarding the examination process from cyber threats, thereby ensuring fair and credible assessments for all candidates.

12.1 Objectives:

(a) Prevention of Cyber Attacks

- The Centre implements robust cybersecurity measures to prevent unauthorised access, data breaches, and any form of interference during the examination process.
- Regular security audits and assessments are conducted to identify and address potential vulnerabilities and include:
  - (i) Applying web filtering and monitoring to include control on devices and networks to block malicious sites and alert suspicious activity; enabling additional security settings wherever possible;
  - (ii) monitoring accounts and regularly reviewing account access, including removing access when no longer required; updating any passwords that may have been exposed; setting up secure account recovery options;
  - (iii) Maintaining a register of all devices and user accounts used for exams and assessment purposes; reviewing and managing connected applications;
  - (iv) ensuring authorised members of staff securely access awarding bodies' online systems in line with awarding body regulations regarding cyber security and the JCQ document Guidance for centres on cyber security: https://www.jcq.org.uk/exams-office/general-regulations
  - (v) Authorised School staff will have access, where necessary, to a device which complies with awarding bodies' multi-factor authentication (MFA) requirements.

(vi) The School will ensure that candidates' work and centre-assessed work are backed-up on two separate devices, including one off-site back-up, thus protect candidates' work in the event of IT system corruption and cyber-attacks.

(vii) Requirements to verify third-party and cloud supplier, meet cyber-security standards and have a data processing agreement in place before use.

(viii) Requirements for assessment administration systems to be included in disaster recovery and business continuity plans, with annual testing of recovery process.

(b) Incident Response

- The Centre will ensure that candidates' work is backed-up on two separate devices, including one off-site back-up, thus protect candidates' work in the event of IT system corruption and cyber-attacks.
- In the event of a cyber attack or suspected breach, the Centre will produce a comprehensive incident response plan. This will include prompt identification, containment, eradication, recovery, and lessons learned.

(c) Communication and Transparency

- Transparent communication will be maintained with relevant stakeholders, including candidates, parents and Centre staff, to keep them informed about any cyber attacks and the steps being taken to address them.
- Updates will be provided in a timely manner, ensuring clarity and confidence in the examination process.

(d) Collaboration with the JCQ and Cambridge

- The Centre will collaborate closely with the JCQ and Cambridge to stay informed about the latest security guidelines and best practices.
- Training sessions may be organized as required to keep Centre staff updated on the evolving threat landscape and effective security measures.
- The Centre will report any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body.

12.2 Responsibilities:

(a) Centre Senior Leadership

- The Centre senior leadership team will take ultimate responsibility for the implementation and adherence to this policy.
- Adequate resources will be allocated to ensure the effectiveness of cybersecurity measures.

(b) Centre Examination Staff

- All Centre examination staff will undergo any training in place on cybersecurity awareness and protocols.
- Authorised School staff are constantly reminded on the importance of creating strong unique passwords and keeping all account details secret; they are also made aware of various types of social engineering/ phishing attempts;
- Centre Staff members are responsible for reporting any suspicious activity immediately.

(c) Candidates/Students

- Candidates/Students are expected to adhere to ethical behaviour during examinations and report any irregularities.
- Unauthorised attempts to access examination systems will be treated seriously and may result in disciplinary action.

13. Review and Updates

This policy is reviewed annually to ensure its relevance and effectiveness in the face of evolving cybersecurity threats. Updates may be made in response to changes in technology, regulations, or examination practices.

14. Maintaining Security

The School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems.