LYCÉE FRANÇAIS CHARLES DE GAULLE DE LONDRES
ICT AND INTERNET ACCEPTABLE USE POLICY

Date of Review: September 2024
Next Review: September 2026

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

TABLE OF CONTENTS

1. Introduction and aims
2. Relevant legislation and guidance
3. Definitions
4. Unacceptable use
5. Staff (including the proprietor's representative, volunteers, and contractors)
6. Pupils
7. Parents/carers
8. Data security
9. Protection from cyber attacks
10. Internet access
11. Monitoring and review
12. Related policies

Appendix 1: Risks of publishing posts on websites and/or via social media
Appendix 2: Social Media cheat sheet for staff
Appendix 3: Acceptable use of the internet and social media: What is expected from parents/carers
Appendix 4: Acceptable use of the School's ICT facilities and internet by secondary school pupils: agreement for pupils and their parents/carers
Appendix 5: Acceptable use of the School's ICT facilities and internet by primary school pupils: agreement for pupils and their parents/carers
Appendix 6: Acceptable use of the School's ICT facilities and internet: agreement for staff, the proprietor's representative, volunteers and visitors
Appendix 7: Glossary of cyber security terminology

This is the ICT and Internet Acceptable Use Policy of Lycée Français Charles de Gaulle de Londres (the "School").

This policy applies to the School's four sites, to all pupils of the School who work with ICT Facilities, and all members of the School community (including without limitation staff, parents and visitors) referred to in this policy.

Mission

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.

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way the School works, and is a critical resource for pupils, staff (including the senior leadership team), the proprietor's representative(s), volunteers and visitors It supports teaching and learning, and the pastoral and administrative functions of the School.

However, the ICT resources and facilities our School uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of the School ICT resources for staff (including the senior leadership team), pupils, parents/carers and the proprietor;
- Establish clear expectations for the way all members of the School community engage with each other online;
- Support the School's policies on data protection, online filtering and monitoring and safeguarding and child protection;
- Prevent disruption that could occur to the School through the misuse, or attempted misuse, of ICT systems;
- Support the School in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our School's ICT facilities, including proprietor representatives, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our relevant School Rules (of the relevant primary School or of the secondary School), behaviour and discipline policy (primary or secondary), and all applicable staff code of conduct policies (including the staff handbook and staff behaviour policy).

2. Relevant legislation and guidance

This policy has regard to the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- The current version of Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges
- www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education
- www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/

3. Definitions

ICT facilities:	all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the School's ICT service
Users:	anyone authorised by the School to use the School's ICT facilities, including staff, pupils, the proprietor representative, volunteers, contractors and visitors
Personal use:	any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
Authorised personnel:	employees authorised by the School to perform systems administration and/or monitoring of the ICT facilities
Materials:	files and data created using the School's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 7 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the School's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the School's ICT facilities includes:

- Using the School's ICT facilities to breach intellectual property rights or copyright
- Using the School's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the School's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Sharing confidential information about the School, its pupils, or other members of the School community
- Connecting any device to the School's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the School's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the School's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities
- Causing intentional damage to the School's ICT facilities
- Removing, deleting or disposing of the School's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the School
- Using websites or mechanisms to bypass the School's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard) as specified in 4.3.

This is not an exhaustive list. The School reserves the right to amend this policy, including this list at any time. The senior leadership team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the School's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of School ICT facilities (on the School premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Proviseure's discretion.

In relation to the acceptable use of Artificial intelligence (AI) tools, please refer to 4.3.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the respective School's policies.

4.3 Artificial intelligence (AI) tools

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. LFCG recognises that AI has many uses to help pupils learn, but may also lend itself to cheating and plagiarism

Pupils may use AI tools:

- As a research tool to help them find out about new topics and ideas

- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

Pupils may NOT use AI tools:

- During assessments, including internal and external assessments and coursework

- To write their homework or class assignments, where AI-generated text is presented as their own work

The School considers any unattributed use of AI-generated text or imagery to be plagiarism and will be subject to sanctions in line with the behaviour and discipline policy

5. Staff (including the proprietor's representative, volunteers, and contractors)

5.1 Access to School ICT facilities and materials

a. Access to School ICT facilities

The School's IT Manager manages access to the School's ICT facilities and materials for School staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the School's ICT facilities.
Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT manager or their deputy.

All requests for access to files must be made by email to support@lyceefrancais.org.uk by the file manager in order to give access to a colleague.

When using the School's ICT facilities and internet, Staff (including the proprietor's representative, volunteers, and contractors) are expected to comply with the expectations listed in Appendix 6, and sign the corresponding form.

b. Use of email

The School provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

All work-related business should be conducted using the email address the School has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

The School provides staff with a guide on the use of emails.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer immediately (via an email sent to dpo@lyceefrancais.org.uk) and follow the Data Protection Officer's instructions on data breach.

c. Use of phones

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the School to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in this section 4.
Staff who would like to record a phone or video meeting conversation should contact the IT Support team (support@lyceefrancais.org.uk). All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to use the School ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Proviseure may withdraw or restrict this permission at any time and at their discretion.
Personal use is permitted provided that such use:

- Does not take place during contact time or teaching/working hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the School's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the School's ICT facilities for personal use may put personal communications within the scope of the School's ICT monitoring activities (see section 5.5). Where breaches of this policy or any other policy of the School are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using the School ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the School's guidelines on use of social media (see appendix 1) and use of email (see section 5.1.(b)) to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The School has guidelines for staff on appropriate security settings for social media accounts (see appendix 2).

5.3 Remote access

The School allows administrative staff and teachers access to the School's ICT equipment and authorised staff are able to use the equipment remotely.

They must connect using a TeamViewer. The remote access system is managed by the IT Support Team.

The remote access uses TCP and UDP protocols.

All requests for remote access must be made by email to support@lyceefrancais.org.uk with prior approval of the Proviseure.

Staff accessing the School's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the School's ICT facilities outside the School and must take such precautions as the IT manager or Proviseure may require against importing viruses or compromising system security.

The School's ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the School's data protection policy.

5.4 School social media accounts

The School has official Facebook, X (formerly Twitter), Instagram, LinkedIn and Youtube accounts, managed by the School's Communications team. Staff members who have not been authorised to manage, or post to, the School's account(s), must not access, or attempt to access, the accounts.

5.5 Monitoring and filtering of the School network and use of ICT facilities

The School reserves the right to filter and monitor the use of its ICT facilities and network in order to prevent or detect crime or comply with a subject access request, Freedom of Information Act request, or any other legal obligation . To safeguard and promote the welfare of children and provide them with a safe environment to learn, the School also monitors the children's ICT use in order to:

- Investigate compliance with School policies, procedures and standards
- Ensure effective School and ICT operation

The proprietor's representative is responsible for making sure that:

- The School meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- The effectiveness of the School's monitoring and filtering systems are reviewed in termly safeguarding meetings and biannual safeguarding committee meetings including the proviseure, the proprietor's respresentative and the designated Safeguarding Lead

The School's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the School's DSL and IT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the School are available to younger (primary, college and Y10) pupils only under the supervision of staff

- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the School's virtual learning environment, which they can access from any device by using the following URL "[https://1320002k.index-education.net/pronote/eleve.html]
- From *seconde* or Y11 (British Section) pupils can use the computers in the CDI, Foyer, Vie Scolaire independently, for educational purposes only.

When using the School's ICT facilities and internet,

- Secondary school pupils (collège, lycée, Y10-Y13) are expected to comply with the expectations listed in Appendix 4 and sign the corresponding form
- Primary School pupils are expected to comply with the expectations listed in Appendix 5 and sign the corresponding form

6.2 Search and deletion

Searching a pupil

French law precludes School staff searching a pupil. If however it is suspected that a pupil is concealing a prohibited item and has refused to hand it over, the pupil will be kept in isolation and the parents/carers will be requested to come to the School in order to search their child. The member of staff must have reasonable grounds to suspect that a device:

- Poses a risk to staff or pupils, and/or
- Is identified in the School rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

If the pupil refuses this parental search, the School reserves the right to contact the Police. In any meeting with an external agency involved in searching a pupil without parental presence, the School will ensure an appropriate adult is present to support the interests of the child.

Under the Education Act 2011, the Proviseure, and a member of staff authorised to do so by the Proviseure, can apprehend pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the School or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the Designated Safeguarding Lead and Proviseure to decide on a suitable response. If there are images, data or files on the device that staff

reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or the pupil and/or the parent refuses to delete the material themselves
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
    - Not view the image
    - Not copy, print, share, store or save the image
    - Confiscate the device and report the incident to the Designated Safeguarding Lead (or deputy) immediately, who will decide what to do next. The Designated Safeguarding Lead (DSL) will make the decision in line with the Department for Education's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the School complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of School

The School will sanction pupils, in line with the applicable behaviour and discipline policy (primary or secondary), if a pupil engages in any of the following **at any time** (even if they are not on School premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the School's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Sharing confidential information about the School, other pupils, or other members of the School community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities
- Causing intentional damage to the School's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the School's ICT facilities as a matter of course.

However, parents/carers working for, or with, the School in an official capacity (for instance, as a volunteer or as a member of the parent teacher association (currently the APL)) may be granted an appropriate level of access, or be permitted to use the School's facilities at the Proviseure's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the School online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the School through our website and social media channels.

Parents are expected to comply with the expectations listed in Appendix 3.

7.3 Communicating with parents/carers about pupil activity

Parents/carers may seek any support and advice from the School to ensure a safe online environment is established for their child. The School's monthly newsletter also informs parents/carers about any local or national related issues.

8. Data security

The School is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the School's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in Schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the School's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Any pupil requests to re-set passwords should be made via vie scolaire who will liaise with the IT team

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the School's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the School's ICT facilities.

Any personal devices using the School's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the School's data protection policy.

8.4 Access to facilities and materials

All users of the School's ICT facilities will have clearly defined access rights to School systems, files and devices.

These access rights are managed by the Proviseure and the IT manager

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert immediately the IT Manager.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day unless working remotely via Teamviewer..

8.5 Encryption

The School makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access School data, work remotely, or take personal data (such as pupil information) out of School if they have been specifically authorised to do so by the Proviseure.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Proviseure and the IT manager.

9. Protection from cyber attacks

Please see the glossary (appendix 7) to help you understand cyber security terminology.

The School will:

- Work with proprietor representative and the IT department to make sure cyber security is given the time and resources it needs to make the School secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the School's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the School will verify this using a third-party audit (such as 360 degree safe) annually to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the School needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data daily automatically and store these backups ever six weeks on an external drive in the School safe by the IT support team
- Make sure staff:
  - Dial into our network usingTeam viewer) when working from home
  - Enable multi-factor authentication where they can, on things like School email accounts
- Make sure ICT staff conduct regular access reviews to make sure each user in the School has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- In case of communications going down, from an IT perspective, continuity will be ensured via a 5G access point and by connecting appropriate professional phones to any of our ICT devices. The IT manager will contact the Proviseure and the proviseurs adjoints and the data protection officer by phone or text. The Data protection officer may notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, the School may refer via the NCSC's 'Exercise in a Box'

10. Internet access

The School's wireless internet connection is secure.

- All School devices using WIFI use web filtering provided by our internet service provider.
- We use separate connections for staff/pupils/parents or carers/public.

- If inappropriate sites are reported or appropriate sites that have been filtered in error, the ICT team will immediately report this to our service provider to block or unblock these sites and the Designated Safeguarding Lead.

10.1 Pupils

Pupils are not allowed to use the School Wifi on their own devices. They should use School-owned devices such as the laptops or tablets available when using the internet at School.

10.2 Parents/carers and visitors

Parents/carers and visitors to the School will not be permitted to use the School's WiFi unless specific authorisation is granted by the Proviseure.

The Proviseure will only grant authorisation if:

- Parents/carers are working with the School in an official capacity (e.g. as a volunteer or as a member of the APL)
- Visitors need to access the School's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on USB as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Proviseure and IT manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the School.

This policy will be reviewed every 2 years.

12. Related policies

This policy should be read alongside the School's following policies:

- Online safety: Filtering and Monitoring policy
- Use Social media: Risk of publishing posts on website and/or via social media
- Safeguarding and Child Protection Policy
- Pupil Behaviour and discipline policies (for the primary schools and secondary school respectively)
- all applicable staff code of conduct policies (including the staff handbook and staff behaviour policy).
- Data protection policy
- IT and Digital Charter, which complements this policy and meets French requirements
- Cybersecurity Policy

Appendix 1: Risks of publishing posts on websites and/or via social media

The Proviseure and Senior Leadership team of the Lycée Français Charles de Gaulle de Londres are aware of the possibility of posts being made on websites and/or via social media about our students or members of staff and the risk that such posts may be offensive. We wish to provide you with information about the risks of making such posts, and your options for responding to any posts which you find offensive:

- Any person who makes postings which harass others, or are defamatory of them, may be subject to criminal and/or civil action. Such posts can be reported to the website operator, the Police, and/or may be the subject of a civil claim for damages and an injunction.

- Private legal action can be taken by any parent who feels that their child has been the target of harassment or defamatory comments.

- The Lycée reserves the right to take very strong measures including the exclusion of any student identified as being the source of harassment or defamatory comments.

- The identity of posters need not remain anonymous. A Court Order can be obtained to reveal the identity of a person responsible for such a post. This allows private legal action to be taken against that person. The Police also have powers to obtain information from website operators if they consider that criminal acts may have taken place.

If your children are considering making use of such websites and/or social media, we ask that you carefully consider with them the potential impact and effect of any post before making it, and ensure that it is respectful and lawful.

Appendix 2: Social media cheat sheet for staff

11 rules for School staff

1. **Do not accept friend requests from pupils on social media**
2. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
3. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
4. Check your privacy settings regularly
5. Be careful about tagging other staff members in images or posts
6. Don't share anything publicly that you wouldn't be happy showing your pupils
7. Don't use social media sites during School hours
8. Don't make comments about your job, your colleagues, our School or your pupils online – once it's out there, it's out there
9. Don't associate yourself with the School on your profile (e.g. by setting it as your workplace, or by 'checking in' at a School event)
10. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
11. Consider uninstalling the social media from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – .e.g. for Facebook, go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – e.g. for Facebook, go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Proviseure about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the School
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 3: Acceptable use of the internet: what is expected from parents/carers

Acceptable use of the internet and social media What is expected from parents/carers
Online channels are an important way for parents/carers to communicate with, or about, our School. The School uses the following channels: ● The School's official Facebook/ Instagram/ Youtube/X (formerly Twitter)/LinkedIn pages ● Email/text groups for parents (for School announcements and information) ● The School's virtual learning platform (Google Classroom) and Pronote Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
When communicating with the School via official communication channels, or using private/independent channels to talk about the School, Parents/carers will: ● Be respectful towards members of staff, and the School, at all times ● Be respectful of other parents/carers and children ● Direct any complaints or concerns through the School's official channels, so they can be dealt with in line with the School's concerns and complaints policy Parents/Carers will not: ● Use private groups, the School's social media pages, or personal social media to complain about or criticise the School or members of staff. This is not constructive and the School can't improve or address issues unless they are raised in an appropriate way ● Use private groups, the School's social media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. Parents/carers will contact the School and speak to the appropriate member of staff if they are aware of a specific behaviour issue or incident ● Upload or share photos or videos on social media of any child other than their own, unless they have the permission of the other children's parents/carers

Appendix 4: Acceptable use of the School's ICT facilities and internet by secondary school pupils: agreement for pupils and parents/carers

Acceptable use of the School's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the School's ICT facilities and accessing the internet in School, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break School rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the School's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
  - During assessments, including internal and external assessments, and coursework
  - To present AI-generated text or imagery as my own work

I understand that the School will monitor the websites I visit and their use of the School's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the School's ICT systems and internet responsibly.

I understand that the School can discipline me if I do certain unacceptable things online, even if I am not in School when I do them.

Signed (pupil): **Date:**

Parents/carer agreement: I understand and agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of School staff. I agree to the conditions set out above for pupils using the School's ICT systems and internet, and for using personal electronic devices in School, and will make sure my child understands these.

Signed (parent/carer): **Date:**

Appendix 5: Acceptable use of the School's ICT facilities and internet by primary school pupils: agreement for pupils and parents/carers

Acceptable use of the School's ICT facilities and internet by primary pupils: agreement for pupils and parents/carers

Name of pupil:

When I use the School's ICT facilities (like computers and equipment) and go on the internet in School, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break School rules
- Go on any inappropriate websites
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work

I understand that the School will check the websites I visit and how I use the School's computers and equipment. This is so that the School can help keep pupils safe and make sure they are following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a School computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when they use the School's ICT systems and internet.

I understand that the School can discipline me if I do certain unacceptable things online, even if I am not in School when I do them.

Signed (pupil): **Date:**

Parents/carer agreement: I understand and agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of School staff. I understand the conditions set out above for pupils using the School's ICT systems and internet, and for using personal electronic devices in School, and will make sure my child understands these.

Signed (parent/carer): **Date:**

Appendix 6: Acceptable use of the School's ICT facilities and internet: Agreement for staff, the proprietor's representative, volunteers and visitors

Acceptable use of the School's ICT facilities and the internet: Agreement for staff, the proprietor representative, volunteers and visitors

Name of staff member/proprietor representative/volunteer/visitor:

When using the School's ICT facilities and accessing the internet in School, or outside School on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the School's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the School's network
- Share my password with others or log in to the School's network using someone else's details
- Share confidential information about the School, its pupils or staff, or other members of the community unless of a safeguarding nature
- Access, modify or share data I am not authorised to access, modify or share
- Promote any private business

I understand that the School monitors the websites I visit and the School's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside School, and keep all data securely stored in accordance with this policy and the School's data protection policy.

I will let the designated safeguarding lead (DSL) and IT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if they encounter any such material.

I will always use the School's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed staff member/proprietor representative/volunteer/visitor:

Date:

Appendix 7: Glossary of cyber security terminology

These key terms will help the School community to understand the common forms of cyber attack and the measures the School will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.