

Langley Grammar School

Online Access & Safety Policy

September 2025



1. Introduction

This policy applies to all students, employees, volunteers, workers or self-employed contractors who may have access to, or use of, IT facilities at the School. For members of staff, adherence to this policy forms part of the School's terms and conditions of employment.

For the purpose of this policy, IT facilities are defined as meaning Langley Grammar School's IT hardware and software, including email, the Internet and other networks, remote access services, and all computers, laptops, iPads or other tablet devices, mobile phones, and any other related applications and devices.

This policy will also apply to:

- any devices owned by students, parents or staff which are brought on to the school site and used to connect to the school network or wifi;
- the use of any new technology being introduced which is not currently detailed in this document.

2. Monitoring and privacy

The School acts in accordance with applicable legislation and the Information Commissioner's Employment Practices Code; notably in relation to the monitoring of communications.

The School undertakes routine monitoring of activity on the IT facilities to ensure that they operate correctly and to protect against the risk of harm from viruses, malicious attack and other known threats. This does not normally involve the monitoring of individual communications or the disclosure of the contents of any user files.

However, the School reserves the right to monitor all staff and student use of the IT facilities, including emails sent and received, and websites and other online content accessed in order to:

- ensure the proper safeguarding of students, minimising exposure to violence, pornography, extremist views and risk of radicalisation;
- protect the IT facilities against viruses, hackers and other malicious attack;
- assist in the investigation of breaches of this policy, to prevent or detect crime or other unauthorised use of the IT facilities;
- comply with legal requirements, for example as part of a police investigation or by order of a court of law, or where necessary as part of a disciplinary investigation.
- pursue the School's other pressing academic and business interests; for example, by reviewing the emails of employees on long-term sick leave or to disclose documents under the Freedom of Information Act 2000.

In all cases, monitoring of individual staff content shall only be carried out if authorised by the Headteacher.

3. Disciplinary regulations and enforcement

Langley Grammar School may take disciplinary action against students or staff if their use of the IT facilities are in breach of this policy.

Where any allegation of misuse has been made against a member of staff or student, the School shall have the right to inspect and take copies of any material held in the name of that student or staff member on any of the IT facilities that might provide evidence for or against the allegation.

If a complaint or allegation is received, a member of staff or student's user account(s) may be immediately suspended for investigation. Wherever possible, users will be notified of such suspension. Penalties for breach of this policy may include temporary or long-term suspension of access to the IT facilities. Other disciplinary penalties may be imposed in accordance with the School's relevant procedures up to and including permanent exclusion in the case of a student, or dismissal in the case of staff. The School may refer the user to the police where appropriate and will co-operate fully with any police investigations.

4. Commercial Activities

Commerce risks include (but are not limited to) online gaming, inappropriate advertising, phishing and financial scams. Use of the IT facilities for commercial activities is permitted only by employees of Langley Grammar School and only when such use forms part of the duties of employment. Any queries on whether a commercial activity using the IT facilities is permitted should be raised with appropriate line managers before commencing.

The use of the IT facilities by students for commercial activities is not permitted.

5. Use of the Internet

The Internet is an essential element of 21st Century life for education, business and social interaction; the School has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the school curriculum and a necessary tool for staff and students. Students will be taught what Internet use is acceptable and what is not and given clear objectives for internet use within their learning. Students will be educated in the effective use of the internet for research, including the skills of location, retrieval and evaluation; they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The School Internet access will include appropriate filtering. However, if internet research is set for a class activity or homework using specific/suggested websites, these must have been checked by teachers or other relevant staff to ensure that they are suitable. The School will also ensure that the use of Internet derived materials by staff and students complies with copyright law.

6. Managing Internet Access

a) Information system security

- School IT systems, capacity and security will be reviewed regularly. Virus protection will be updated regularly. Whilst there are IT security systems in place, the School cannot guarantee that these will prevent every attempt to access confidential or restricted data.
- Users should ensure that confidential data is stored securely and is used appropriately, whether in school, or when taken off the School premises according to the most recent GDPR legislation at a minimum, plus any additional requirements from the school
- The school does not permit the storage of personal data on USB sticks or external drives unless they are encrypted. Staff and students are generally discouraged from using USB sticks.

b) Social networking and personal publishing

- The School will block/filter access to inappropriate social networking sites.
- Students will be advised never to give out personal details online which may identify them or their location.
- Students and parents will be advised about the risks of using social network spaces outside School.
- There must be no contact between staff and students on social networking sites using personal identities, including pseudonyms or nicknames.
- Any online contact between staff and students must only be through the use of school email addresses or approved, appropriate applications.
- Staff are made aware of expectations with regard to their personal use of social media within the general Staff Code of Conduct.
- All staff additionally complete a declaration to confirm that they have read and will adhere to the Staff ICT Acceptable Use Agreement (see Appendix D) to ensure safe practices with regard to the use of the school IT systems, the internet and social networking.
- The ICT Acceptable Conduct Agreement reinforces the safe and sensible use of all IT equipment and services including the Internet and social media. A copy of the agreement can be found on students' iPads.

c) Managing filtering

- The School will work with its contracted provider of filtering services to ensure systems to protect students are regularly reviewed and where necessary, updated.
- Staff or students will be reminded that if they discover an unsuitable site, it must be reported to the Safeguarding Team..
- Senior staff and the ICT technicians will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and robust.

d) Managing emerging technologies

- Emerging technologies will be examined for educational benefit; the Safeguarding Team alongside SLT will review the risks before use in School is allowed.

e) Mobile phones

- Students in Year 7 -11 may only use mobile phones before and after school; Sixth Form students may use their mobile phones in the Sixth Form Centre.
- The sending of abusive or inappropriate messages or other forms of communication is unacceptable.
- Unacceptable or inappropriate use of mobile phones by students will result in confiscation and may result in the imposition of other sanctions.
- Staff must not share their personal mobile phone numbers with students.

f) iPads

- Students use iPads to support their learning throughout Years 8 to 11 and in the Sixth Form; Year 7 have introductory sessions with their iPads towards the end of Year 7.
- Students in Year 8 -11 may only use iPads before and after school and during lunchtime; Year 7 can only use iPads when authorised by their teachers.
- All students must adhere to the iPad User Agreement (see Appendices) which sets out some specific principles for iPad use in lessons and social time. A copy of the agreement for Years 7 to 11 is on their iPads and a copy is in the Welcome Pack for students in the Sixth Form.
- Regardless of funding source, as part of the use agreement all devices are connected to the school's mobile device management system which imposes certain appropriate restrictions on use while in school and/or at home.

g) Protecting personal data

Personal data will be recorded, processed, transferred and made available with due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- Data Protection Act (2018).

7. Handling online safety complaints

- Complaints of IT misuse by students will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection or safeguarding nature must be dealt with in accordance with School Safeguarding and Child Protection policy.
- Complaints related to Data Protection must be dealt with in accordance with the Schools' Data Protection Policy.

8. Education

The school will ensure that students are taught about online safety. This will involve the topic being embedded across a range of subjects and experiences.

A number of online safety themes such as Youth Produced Sexual Imagery and online grooming will be delivered through Sex and Relationships Education (SRE) and via the pastoral programme.

9. Staff training

Staff will be trained to understand how to advise students on how to stay safe online. They will be updated regularly on emerging trends and the risks involved.

10. Monitoring and review

The implementation of this policy will be monitored and evaluated by the Senior Leadership Team and the Governors' Student and Community Committee as part of the review of safeguarding arrangements.

The policy will be reviewed in line with the LGS policy framework; this review will take place every two years or whenever there is a significant change in national guidance on online safety.

Ratification and review dates

Reviewed by:	Headteacher	Date:	August 2025
Approved by:	Headteacher	Date:	September 2025
Next review due:	June 2027		

Appendix A

ICT Acceptable Use Policy for Students

Online Safety and the use of ICT is an important commitment at Langley Grammar School. Therefore, we have high expectations of students to maintain the highest standards of sensible and safe behaviour. This agreement outlines within its rules what we expect from students to support themselves and other students' safe usage of ICT equipment (including personal digital devices such as mobile phones and tablets), the internet and technology services at the school.

Expectations
<ol style="list-style-type: none">1. I will use IT systems including the data, internet, email, digital video and mobile technologies, in a safe and respectful manner.2. I will not use a personal digital device, e.g. mobile phone, during the school day unless requested or approved by staff.3. I will not attempt to change, misuse or damage the features or behaviour of school systems and data. This includes, but is not limited to, creating, downloading or installing software, malware or any unapproved code on school systems.4. I will only log on to the school network/accounts with my own school username and password.5. I will not use anyone else's username and password6. I will not access anyone else's data if not authorised.7. I will not reveal my passwords to anyone other than appropriate members of staff.8. I will not attempt to damage, undermine or breach school security systems on the network infrastructure or internet including attempting to bypass the internet filtering system.9. I will make sure that all IT communication with students, teachers or others are responsible and sensible.10. I will use only my school email address to communicate with members of staff.11. I will not use my personal social media accounts to communicate with members of staff.

12. I will not use the internet to access inappropriate resources. I will follow the guidance and advice of any member of staff.
13. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. This includes any material of a violent, racist, dangerous, pornographic or other inappropriate nature including that which promotes extremism and radicalisation.
14. I will be polite and respect that other users might have different views. I will not state anything which could be interpreted as libel. I will not write offensive, racist, sexist, abusive, homophobic or aggressive words.
15. When using public networks such as the Internet, I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by a member of staff.
16. I will regularly check my privacy settings on social media sites to make sure they are up to date and effective.
17. I will let a member of staff know immediately if I am sent anything I do not feel comfortable about.
18. I will not store inappropriate or indecent images (which may include personal images) on school or personal digital devices. I will not distribute such images and understand that both these actions are potentially illegal.
19. I understand that I must not take, edit or make digital images, sound recordings or video footage of any of the school's students or staff without clear permission from the school and the person/s involved.
20. I understand that all computer storage areas (including any external storage media I bring to school) will be available for appropriate school staff to review files and usage.
21. I understand that appropriate school staff have the right to view any digital communications made using school systems to ensure the use of such systems is responsible and appropriate.
22. I understand that the school will treat cyberbullying as a serious issue. Bullying using social networks, texting, video or any other electronic media to harass, intimidate or upset somebody will result in disciplinary actions.

23. I will not create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to others.
24. No images, recordings or videos that could bring the school into disrepute should be distributed via electronic media including social networks and video service providers. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school into disrepute.
25. Due to issues of copyright, I will not allow or cause my or another students' original work to be used to train generative AI models.
26. Due to issues of data protection, I will not input personal data (i.e. any information relating to an identified or identifiable person) into any AI platform (e.g. ChatGPT).
27. While a student at this school, I agree to adhere to the Online Safety and Access Policy, including this ICT Acceptable Use Agreement.

In addition, when using an iPad, I agree to the following expectations:

1. In lessons leave your iPad in your bag until you've been asked to use it by a teacher;
2. When using your iPad in lessons, it must be flat on the table or slightly raised;
3. Your iPad should be passcode protected;
4. Each day there should be enough memory and battery life for your schoolwork;
5. You must bring a tablet stylus to school each day (marked with your name);
6. In lessons, you should be on task and using your iPad appropriately at all times – if not sanctions will be strictly applied;
7. At the start of PE/Games lessons, lock the iPad away in the PE lockers provided;

8. During lunchtimes your iPad should be in your bag and with you at all times. If this is not possible, it should be locked in your personal locker;
9. Always keep your work backed up to 'One Drive' or similar cloud storage;
10. You must check your school email at least once every 24 hours during the school week;
11. For your own safety, you are advised NOT to use your iPad in public places such as nearby parks or on public transport.
12. Any iPad used in school must have mobile device management software installed on it.
13. You must not use VPNs at any time, or mobile hotspots during school hours, on your iPad.
14. Your iPad should always be connected to the school wifi with your own username and password.

Appendix B

Policy on the use of personal computers by Sixth Form students on school premises

Aside from our use of iPads as a school, the school does not recommend the use of personal computers in school. It provides antivirus, ICT support and other security measures automatically and free of charge on school computers, whereas individuals are responsible for maintaining security and ICT support, at their own cost, on personal computers.

However, if Sixth Form students do bring a personal computer to school, they agree to:

- Purchase an antivirus with an active licence;
- Keep device firewall turned on;
- Have an operating system where the manufacturer is still providing security updates;
- Apply all critical operating system updates (Windows, Mac or Linux updates);
- Apply all software updates and not use software that is not supported by the manufacturer;
- Connect to the school's wifi only, and only for the purposes of your studies;
- Only use your laptop during private study and not in lessons;
- Take all possible steps to proactively protect the school's network and its data, and your own data, and follow the school's acceptable use policy for ICT.

Recommendations for keeping laptop secure:

- <https://www.ncsc.gov.uk/guidance/end-user-devices-advice-end-users>

How to check if whether an operating system is supported with security updates:

- <https://support.apple.com/en-us/HT201222>
- <https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet>
<https://linuxlifecycle.com>

Appendix C

Notices for Parents

For Parents:

By enrolling your child at Langley Grammar School, you grant permission for your child to use email and the internet.

You understand they will be held accountable for their own actions.

You also understand that some materials on the internet may be objectionable and accept responsibility for setting standards for your child to follow when selecting, sharing and exploring information and media from home.

You agree you have read and understand the school's Online Access & Safety Policy (most recent version on the school website).

You also agree that you are responsible for purchasing the relevant insurance policies for electronic devices and accessories brought to school premises, including iPads, mobile phones, headphones etc. This is regardless of purchasing model, e.g. purchased by or leased from school, or independent purchase by us. The school does not accept liability for any losses or damages incurred.

Appendix D

Langley Grammar School

Staff Acceptable ICT Use Agreement

September 2025



Background

The school will try to ensure that staff will have good access to digital technology to enhance their work, and to improve the effectiveness of students' learning. In return, the school expects staff to agree to be responsible users of that technology.

This Acceptable Use Agreement is therefore intended to ensure:

- that staff will be responsible users and stay safe while using the school's information communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk through their use of technology in their everyday work.

All members of staff are required to read this Acceptable Use Agreement to ensure they are fully aware of their professional responsibilities when using ICT and when communicating with students.

Staff should consult the school's Online Access and Safety Policy (which can be found on the school's website) for additional information and clarification.

If a member of staff is unsure about what is expected of them, they should speak to their line manager in the first instance or a senior member of staff to seek clarification. All members of staff must confirm that they have read, understood and accept this Acceptable Use Agreement as part of their induction, and typically on an annual basis thereafter.

Acceptable ICT Use Agreement

I understand that the term Information Communications Technology (ICT) includes a wide range of hardware including desktop PCs, laptops, iPads and other tablet devices, mobile phones, digital cameras, and software systems including email and social networking.

I understand that I must use school ICT systems in a responsible way, to ensure that the potential risks to my safety or to the safety and security of the systems and other users are minimised. I will, where possible, educate the students in my care in the safe use of digital technology and routinely embed considerations of online safety in my work.

For my professional and personal safety...

- a) I acknowledge that any ICT devices provided for me to use remain the property of the school are intended primarily for educational use.
- b) I understand that when using school ICT devices and/or software for personal purposes, such usage must be carried out in accordance with this Acceptable Use Agreement and should not interfere with the discharge of my professional responsibilities.
- c) I will respect system security and will not disclose password or security information to anyone other than an authorised school ICT system administrator. Where possible, I will use multi factor authentication to secure my accounts, change my passwords on a regular basis, and not re-use personal passwords on school accounts.
- d) I will ensure that I do not leave any device unlocked while unattended.
- e) I will follow the guidance provided by the school's ICT technical team to ensure the anti-virus protection on my devices is up-to-date.
- f) I understand that my use of school's digital technology and communication systems, including email and access to the internet, may be monitored and recorded to ensure compliance with school policies.
- g) I will immediately report to the appropriate person any illegal, inappropriate or harmful material or incident that I become aware of.

To ensure that my communications and actions when using school's ICT systems are appropriate and professional ...

- h) I will only communicate with students, parents and other relevant parties using official school systems, and will ensure that any such communication will be professional in tone and manner.
- i) I will not create, transmit, display or publish any material that is likely to harass or cause offence to any other person or bring the school into disrepute.
- j) I will not use the school ICT systems to make disparaging, inflammatory or unprofessional references to the school, its staff, governors, students, families, or any other persons associated with it.
- k) I understand that any social media platforms used to communicate with students must be set up for educational purposes only and must not be used for personal communication. When registering for such sites or platforms, I will use my school email address.
- l) I will not post any information regarding my activities at school, or the school in general on my personal social networking sites. I will be clear that any comments made on social networking sites (e.g. political views) are my own personal opinion. I will not connect with current students or former students with siblings still attending the school through personal social media.
- m) I understand that my use and storage of photographic images or video recordings of students taken in school or on school activities should be compatible with my professional role.

- n) Any images I may take of students using my own personal device (eg mobile phone, camera and/or tablet) will be uploaded to the school's network or cloud storage as soon as possible, and the images deleted from my personal device immediately afterwards.
- o) I understand that use of the school's digital technology and communication systems for personal financial gain, gambling, political purposes or advertising is forbidden.

To ensure that access to digital technology and communication systems is safe and secure...

- p) I understand that data stored appropriately using the school systems is backed up and secure. I acknowledge that data stored elsewhere might not be backed up and that I am responsible for any loss or data breach.
- q) I will immediately report any damage or faults involving school ICT equipment or software, however this may have happened.
- r) I will not install software or hardware on any of the school's ICT systems, my school laptop or iPad without consulting the ICT technical team.
- s) I will ensure that confidential data is stored securely and used appropriately, in accordance with the most recent data protection legislation and any additional requirements made by the school, for example those set out in the Data Protection policy. I will not access or store school data on or through unprotected personal devices, e.g. unencrypted USB sticks or external hard drives.
- t) I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- u) I will report any concerns related to data protection to the school's Data Protection Officer.

When using the internet in my professional capacity...

- v) I will ensure that I have permission to use the original work of others in my own work.
- w) Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- x) Due to issues of copyright, I will not allow or cause students' original work to be used to train generative AI models unless I have the student's permission.
- y) Due to issues of data protection, I will not input personal data (i.e. any information relating to an identified or identifiable person) into an open AI platform (e.g. ChatGPT).

To ensure that students are safeguarded...

- z) I will only use school systems in line with the DfE Filtering & Monitoring Standards and will never attempt to bypass the school's filtering and monitoring controls.
- aa) I will report any filtering or monitoring concerns or suspected weaknesses to the Designated Safeguarding Lead immediately.
- bb) I will report any incidents of concern regarding students' safety to the Designated Safeguarding Lead (DSL) or Headteacher.

cc) I will not ask or allow students to use generative AI tools for school work (in school, at home, or off-site) unless the Senior Leadership Team has explicitly approved such use *and* that appropriate safeguards are in place consistent with the DfE's guidance on the use of Generative AI in education.

I understand that I am responsible for my actions in and out of Langley Grammar School and that, this Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

If I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action and that other consequences may follow. In certain circumstances, this could include investigation by the police or the Information Commissioner's Office, or notification to appropriate professional bodies.

This list is not exhaustive. Above all, in accordance with the Teaching Standards (2012), staff must act professionally at all times and must not, through their actions or inactions, place students at risk of harm or bring the school into disrepute.