Langley Grammar School

Online Access & Safety Policy
May 2021

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 school approved 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 – alerting staff where appropriate.
- 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

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. The School has IT security systems in place but 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 unless they are encrypted. Staff and students are generally discouraged from using USB sticks.
- Year 7 and Year 12 parents and all those that join during any one academic year will be asked to give written consent for students to use the internet in School.

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.
- 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 sign an ICT Acceptable Conduct Code of Conduct (see Appendix E) to ensure safe practices with regard to the use of the school IT systems, the internet and social networking.
- All students will sign the ICT Acceptable Conduct and Online Access & Safety Agreement for students joining the school in 2020-21 (Appendix A-D) which 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 in the student planner.

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 regularly reminded that if they discover an unsuitable site, it must be reported to the ICT technical 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 and a risk assessment will be carried out before use in School is allowed.

e) Mobile devices

- Students may only use mobile phones before and after school and during lunchtime. Sixth Form students are permitted to use 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 may result in confiscation and 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.
- Students in Year 7 -11 may only use iPads before and after school and during lunchtime.
- All students must adhere to the iPad User Agreement (see Appendix C) which sets out some specific principles for iPad use in lessons and social time. A copy of the agreement can be found in the student planner, or equivalent digital documents on the iPad or school website.
- Most students' iPads are parentally funded and owned but 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. Parents sign to indicate their agreement.

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) (replaces the 1998 Data Protection Act)

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 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: how youngsters are using online applications 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.

Policy reviewed:	**May 2021**	**Assistant Headteacher**
Policy reviewed:	**Pending**	**Student & Community Committee**
Policy approved:	**Pending**	**Headteacher**
Next review:	**May 2023**	

Appendix A – Student Information

Policy on the use of personal digital devices on school premises

The school insists that all IT systems and personal digital devices are used for educational purposes during the school day and in an appropriate manner. Any breach of the expectations will be considered a disciplinary matter.

Violations of the above expectations may result in**:**

1. a temporary ban or future restrictions on internet/computer use;
2. additional disciplinary action in line with existing behaviour for learning policy;
3. parents/carers being informed;
4. involvement of the Police.

We believe in personal responsibility, and in enrolling with the school students are accepting responsibility for using the IT equipment, including personal digital devices, the internet and technology services at Langley Grammar School.

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 you are responsible for maintaining security and ICT support, at your own cost, on personal computers.

However, if you (as a Sixth Form student) do bring a personal computer to school, you agree to:

- Provide evidence of having purchased 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;
- 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 your 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 B – Agreements

ICT Acceptable Conduct Agreement

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.

ICT Acceptable Conduct Expectations

1. I will use IT systems including the internet, email, digital video and mobile technologies, in a safe and respectful manner.
2. I must have my parent's/carer's permission before using the internet.
3. I will not download or install software on school electronic devices.
4. I will not attempt to introduce a virus or malicious code on to the network.
5. I will only log on to the school network/Sapientia with my own username and password.
6. I will not use anyone else's username and password or 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 try to 'hack', undermine or breach the 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 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. By signing the declaration I agree to adhere to this agreement and also acknowledge the iPad acceptable use rules that are displayed in student planners and on the school website.

Appendix C

iPad User Agreement

The expectations below run in conjunction with the school's IT Acceptable Conduct Agreement.

1. In lessons leave your iPad in your bag until you've been asked to use it by a teacher;
2. Your iPad should be password protected;
3. Each day there should be enough memory and battery life for your schoolwork;
4. You must bring a stylus to school each day;
5. In lessons, you should be on task and using your iPad appropriately at all times – if not sanctions will be strictly applied;
6. At the start of PE/Games lessons, lock the iPad away in the PE lockers provided;
7. 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;
8. Always keep your work backed up to 'One Drive' or similar cloud storage;
9. You must check your school email at least once every 24 hours;
10. For your own safety, you are advised NOT to use your iPad in public places such as nearby parks or on public transport.
11. Any iPad used in school must have mobile device management software installed on it.
12. You must not use VPNs at any time, or mobile hotspots during school hours, on your iPad.
13. Your iPad should always be connected to the school wifi with your own username and password.

These expectations were recommended by the School Council and approved by the Leadership Team January 2016

Appendix D – Declaration

ICT Acceptable Conduct and Online Access & Safety Agreement for students joining the school

For students:

When using digital technology in school I agree to comply with the rules as laid out in the ICT Acceptable Conduct Agreement (a copy of which is on the school website):

- I will use all ICT resources including the internet, the school's network and any other digital device in a responsible way and observe all the restrictions explained to me by the school, including the enrolment of my iPad on Mobile Device Management and the installation of Internet filtering certificates on any digital device I use
- I confirm that I have also read and understood the school's Online Safety Policy (available from the school website).

Signed: _____

Printed name: _____

Date: _____

(or can be accepted electronically during Admissions process)

For Parents:

As the parent or legal guardian of the student signing above, I grant permission for my son or daughter to use email and the internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media from home. I confirm that I have read and understand the school's Online Safety Policy (available from the school website).

I also agree that we 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.

Signed: _____

Printed name: _____

Date: _____

(or can be accepted electronically during Admissions process)

Appendix E

Langley Grammar School
Staff Code of Conduct for IT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are required to sign this Code of Conduct. Members of staff should consult the School's Online Safety Policy (which can be found on the School's website) for additional information and clarification.

- I appreciate that IT includes a wide range of hardware and software systems, including laptops, tablets, mobile phones, PDAs, digital cameras, email and social networking.
- I understand that when using school IT systems for personal purposes such usage must be carried out in accordance with this Code of Conduct and should not interfere with the discharge of any professional duty.
- I understand that my use of school IT systems, the Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised IT system administrator.
- Where possible, I will use multi factor authentication to secure my accounts, and I will not reuse personal passwords on school accounts.
- I will proactively ensure the confidentiality, integrity and availability of our systems and services, and the personal data we process within them. If an external storage device is a necessity, I will ensure that I only use encrypted devices. I will also apply software updates in a timely manner.
- I will not install inappropriate software or hardware without permission onto any of the School's ICT systems, my school laptop or iPad.
- I will 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 the school places
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding students' safety to the Designated Safeguarding Lead (DSL) or Headteacher.
- If I have a reasonable concern that a student's digital device contains content that may put the student or others in a vulnerable position I may confiscate the device <u>but should not search it</u>. I should hand the device to the Headteacher or the DSL
- I will not allow parents or students to add me as a 'friend', nor will I add them as 'friends', on social networking sites.
- I must be clear that any comments made on social networking sites (e.g. political views) are my own personal opinion.

- I may use social media to communicate with students but such sites/applications must be set up for educational purposes only and must not be used for personal communication. When registering for such sites I will use my school email address.

- I will not place any information regarding my activities at school, or the School in general on my personal social networking sites.

- I will not create, transmit, display or publish any material that is likely to: cause offence, harass, inconvenience or needless anxiety to any other person or bring the School into disrepute.

- 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.

- In addition to the previous point, I further understand that any images I may take of students using my own personal device including a phone, camera and/or tablet should be uploaded to a central location such as the school network as soon as possible. These images should be deleted from my personal device immediately afterwards.

- In line with safeguarding procedures, I will not use the IT system to make disparaging, inflammatory or negative comments that make reference to the School, its staff, governors, students, families, or any other persons associated with it.

- I understand that email communication with students must only be carried out using the school email system.

- I will promote online safety with students in my care and will help them to develop a responsible attitude to IT use, communications and publishing.

- I have read the School's Online Safety Policy.

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, bring the School into disrepute.

The School may exercise its right to monitor the use of IT systems including internet access and e-mail. In addition, authorised persons may delete inappropriate materials where the School believes unauthorised use of its IT systems may be taking place. This includes criminal activity such as storing unauthorised or unlawful text, images or sound.

I have read, understood and accept the Staff Code of Conduct for IT.

Signed: _____

Printed name: _____

Date: _____