

Langley Grammar School

Online Access & Safety Policy September 2016



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 employees, 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 any of 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 or parents which are brought on to the school site;
- 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.

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

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. Everyone must ensure that confidential material is password-protected and / or encrypted as appropriate to prevent unauthorised access by third parties including laptops and hard drives etc.
- 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 Code of Conduct 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 Code of Conduct which reinforces the safe and sensible use of all IT equipment and services including the Internet and social media.

c) Managing filtering

- The School will work with its contracted provider of filtering services to ensure systems to protect students are reviewed and improved.
- If staff or students 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 phones

- Students may only use mobile phones during social time (i.e. before/after school, breaktime/lunchtime). The sending of abusive or inappropriate messages or other forms of communication is forbidden.
- 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 into the Sixth Form.
- All students sign an iPad User Agreement which sets out some specific principles for iPad use in lessons and social time.
- 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.
-

g) Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

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.

8. 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:	Jun 2015	Student & Community Committee
Policy approved:	Jun 2015	Headteacher
Policy revised and reapproved:	Dec 2015	Headteacher
Policy revised and reapproved:	Sep 2016	Headteacher
Next review:	July 2018	