

**Student
Acceptable Use / E-Safety
Policy**
(student version)



THE GRAMMAR SCHOOL
AT LEEDS

Be Inspired

date of previous review: August 2017

date of issue of new policy: September 2017

next review due: August 2018

Contents

1.	Introduction.....	3
2.	Principles	3
3.	Personal safety.....	4
4.	Using technology as a resource	4
5.	Interacting with others	5
6.	GSAL systems.....	5
7.	When using the internet for research or recreation	5
8.	Responsible for behaviour, both in and out of school.....	6
9.	Email use	6
10.	Personal devices	6
11.	Managing emerging technologies	7

Introduction

The school recognises that digital technology and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Students at GSAL are expected to exhibit good behaviour in their use of the school network just as they are in a classroom or any other learning context provided by the school. Ultimately GSAL owns the computer network and sets both the guidelines for its use and sanctions for misuse. Students should remember that access to computers and the internet is a privilege not a right and that that privilege can be and will be withdrawn at the school's discretion if their behaviour is not in the interest of their learning nor of the community as a whole. Students are expected to respect the equipment provided by school and to abide by the various policies concerning the use of computers at GSAL.

Staff may review files and communication periodically to ensure that students are behaving responsibly on the system.

Violation of the rules below will result in a ban on computer and network use and may include other disciplinary action in accordance with the school's Behaviour Policy and Serious Discipline Procedure Policy. When applicable, the Police or local authorities may be involved.

Principles

Students understand that they must use the school ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users.

Whilst students are expected to adhere to all aspects of this document, specific attention must be drawn to the following guidelines:

- i) Video, audio and photographic recording must never take place without the consent of student(s) and teacher(s). Consent must be explicit, not implied.**
- ii) Social media and messaging are never to be accessed during school time unless as part of a directed teaching activity.**
- iii) The same principles apply when using all platforms and means of access to online activity whilst under the supervision of staff on or off the school site.**
- iv) Malicious or deliberate damage to school, staff or pupil equipment; unauthorised access to the network; theft of hardware, software or data; the introduction of malware or viruses; or any other deliberate actions against GSAL systems will be regarded as a serious breach of school regulations.**

At GSAL, students are:

- Responsible for their behaviour (conduct)
- Aware how they interact with others (contact)
- Safe with the materials they use and create (content)

This policy should be read in conjunction with the following GSAL school policies:

- Anti-Bullying Policy
- Behaviour Policy
- Plagiarism Guide for Students
- Safeguarding Children Policy
- Serious Discipline Procedure Policy
- Searching Electronic Devices Policy

1. Personal safety

- 1.1. Students understand that the GSAL systems are primarily intended for educational use and that they will not use them for personal or recreational use unless they have permission.
- 1.2. Students understand that GSAL will monitor student's use of the systems, devices and digital communications.
- 1.3. Students will keep their username and password safe and secure for any online account. Students will not share it, nor will they try to use any other person's username and password. Students understand that they should not write down or store a password where it is possible that someone may steal it. Try to change passwords on an annual basis at the very least.
- 1.4. Students must be aware of "stranger danger", when communicating online.
- 1.5. Students will not disclose or share personal information about themselves or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details and financial details).
- 1.6. Remember that images and text you post online can be quickly shared or copied by many other people and can't always be taken back.
- 1.7. Never agree to meet anyone you have met online without taking an adult you trust with you – people online are not always who they say they are.
- 1.8. Do not leave any computer unattended with an open (logged on) session. This also applies to remote sessions on portable devices or from home. If students need to leave a computer for a short break, they should lock the session.

2. Using technology as a resource

- 2.1. Students will not try (unless permission has been given by a member of staff) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- 2.2. Students will not use GSAL systems or devices for online gaming, online gambling, internet shopping, file sharing or video broadcasting (eg You Tube), unless permission has been given by a member of staff to do so.
- 2.3. Students are not allowed to access, produce, display, circulate or store pornographic material.

3. Interacting with others

- 3.1. Students will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- 3.2. Students will be polite and responsible when communicating with others; they will not use strong, aggressive or inappropriate language and will appreciate that others may have different opinions.
- 3.3. Students will not take or distribute images of anyone without their permission. Students also know that it is a criminal offence to possess, manufacture or distribute indecent images and video of children (under the age of 18).
- 3.4. Email communication between pupils and staff should always use the school provided email accounts and not personal email accounts.
- 3.5. Anonymous messages and chain letters are not permitted.
- 3.6. If students receive any negative communication and / or inappropriate content, they will report this to computer services, ensuring that the evidence is kept to show them.

4. GSAL systems

- 4.1. Students will only use their own personal devices in school if they have permission from a member of staff. Devices will otherwise be switched off. Students understand that, if they use their own device in school, they will follow the rules set out in this agreement, in the same way as if they were using school equipment.
- 4.2. Students understand the risks and will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others, nor will they use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
- 4.3. Students will immediately report any damage or faults involving equipment or software, however this may have happened.
- 4.4. Students will not open any hyperlinks in emails or any attachments to emails, unless they know and trust the person / organisation who sent the email, or if students have concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- 4.5. Students will not install or attempt to install or store programmes of any type on any school device, nor will they try to alter computer settings.
- 4.6. Students will only use social media sites with permission from a member of staff, and at the times that are allowed.

5. When using the internet for research or recreation

- 5.1. Students should ensure that they have permission to use the original work of others in their own work (see Plagiarism Policy).
- 5.2. Where work is protected by copyright, students will not try to download copies (including music and videos)

- 5.3. When students are using the internet to find information, they should take care to check that the information that they access is accurate, as they understand that the work of others may not be truthful and may be a deliberate attempt to mislead.

6. Responsible for behaviour, both in and out of school

- 6.1. Students understand that GSAL also has the right to take action against them if they are involved in incidents of inappropriate behaviour, that are covered in this agreement, when they are out of school and where they involve their membership to the school community (examples would be online bullying, use of images or personal information).
- 6.2. Students should ensure that their activity online does not bring the school's name into disrepute.
- 6.3. Students understand that if they fail to comply with this Acceptable Use Policy agreement, they will be subject to disciplinary action. This may include amongst other measures loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

7. Email use

- 7.1. All staff/student email communication should use the school provided email accounts and not personal email accounts.
- 7.2. Emails must not contain any inappropriate or abusive text or pictures and any such messages received must be reported to Computer Services immediately.
- 7.3. Emails should be written carefully and politely, particularly as email could be forwarded to unintended readers.
- 7.4. Students should not reply to unpleasant emails.
- 7.5. Students should be wary of email attachments and should not open any which are from an unknown sender or which look suspicious.

8. Personal devices

- 8.1. Students understand the primary purpose of having their personal device at school is educational, irrespective of whether the device is school owned or personal.
- 8.2. Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network. Devices which do compromise the network will be blocked and the associated user account disabled.
- 8.3. Devices may be used in lessons in accordance only with teacher discretion. When devices are not to be used, they should be for example, away in bags or face down on the table.
- 8.4. Students must not connect any device to the wired network.
- 8.5. Students may connect personal devices to the GSAL student WiFi network as per the terms of this policy, and solely in order to further educational development and independent learning. However, those devices are subject to the same restrictions as any other device connected to the network and their use will be monitored.

- 8.6. Student personal devices are brought into school entirely at the risk of the owner and the decision to bring the device in to the school lies with the student and their parents as does the liability for any loss or damage resulting from the use of the device in school.
- 8.7. The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- 8.8. The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- 8.9. The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around school.
- 8.10. Passcodes or PINs must be set on personal devices to aid security.
- 8.11. The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- 8.12. Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's Discipline Policy. Their electronic device may be confiscated. In the event of confiscation the member of staff will make arrangements for its return, which would normally be at the end of the school day.
- 8.13. Video, audio and photographic recording must never take place without the consent of student(s) and teacher(s). Consent must be explicit, not implied.
- 8.14. Social media and messaging are never to be accessed during class time unless as part of a directed teaching activity.

9. Managing emerging technologies

- 9.1. Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have.
- 9.2. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.