



STAFFORD GRAMMAR SCHOOL

Prep 3-11 | Senior 11-16 | Sixth Form 16-19

Digital Policy - Pupils

Policy Review

Date of Review	Reason for Review	Reviewer	Checked & approved	Date of approval	Next review
29.09.25	Annual review	Assistant Head	Headmaster and Safeguarding & Behaviour Governor Committee	29.09.25	29.09.26

Section 1 Bring Your Own Device Acceptable Use Policy (Pupils)

Scope of this Policy

Stafford Grammar School is committed to enabling pupils to use technology to enhance their learning and to support traditional methods of teaching and learning to equip them for the world of work. Bringing their own device will familiarise pupils to work across different platforms and to gain confidence and skills in the use of technology across all subjects.

This policy applies to all pupils who have access to the School's IT systems and to all use of the School's computer systems, including access to those systems using personal devices, and all use of computers (including personal devices) on school property or in connection with school activities.

Pupils using their own devices in School are subject to the conditions of this policy, ICT Security Policy, Student Email Acceptable Use Policy, E-safety Policy, Anti-bullying Policy and Behaviour Policy. Failure to adhere to these conditions may result in disciplinary action as appropriate.

Bring Your Own Device

Stafford Grammar School recognises the importance of technology and the educational benefits available through the use of technology. The use of portable electronic devices in the classroom can add educational value when

such devices deliver content and extend, enhance or reinforce the student learning process.

Pupils in Years 3-13 may access the School's wireless network with an approved mobile personal device. Broadly speaking these devices are classified as tablets or laptop computers with a QWERTY keyboard. Users wishing to use such devices should ensure that they are able to access the School's G Suite provision (including Google Classroom, Gmail, and Google Docs etc.) and that their device meets or exceeds the minimum system requirements for this product.

Pupils in Year 12 and 13 may also access the School's wireless network using a personal mobile phone but these must only be used in the sixth form centre and the student's destination classroom with permission of the classroom teacher.

Pupils will be responsible for setting up and maintaining the devices that they wish to connect to the network.

The wireless network will not provide print services. Internet and email access will be filtered and monitored subject to normal School policy.

Specific Conditions for Using Devices in School:

1. Stafford Grammar School pupils in Year 3 and above are permitted to use their own device in their lessons for educational purposes only when directed by school staff. Playing games or other non-school work-related activities are not permitted.
2. All personal electronic devices brought into the School must be used in a responsible and legal manner and should not cause disruption to the educational environment.
3. The School reserves the right to confiscate and inspect a student's personal electronic device if there is reason to believe that the student has violated School policies or has engaged in other misconduct. On occasion, pupils may reasonably be required to make available for inspection the contents of privately owned online accounts, including smartphone apps.
4. Pupils must access school IT systems using their own username and password.
5. Pupils must not share their username or password with anyone else.
6. Pupils must not attempt to access parts of the school's IT systems which they do not have permission to access, or look for vulnerabilities in the systems.
7. Personal devices must not contain content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is of a pornographic nature, obscene or promotes violence, discrimination or extremism).

8. Pupils are responsible for ensuring the safety of their own personal devices. The School is not responsible for the loss or theft of a device, nor are they responsible for any damage done to the device while at School.
9. Pupils must keep devices turned off when requested.
10. Pupils must ensure that the device has sufficient electrical charge for use as the School cannot guarantee the availability of charging stations.
11. Pupils may not use the camera feature to capture, record, or transmit audio, video or still photos of other pupils, or staff/visitors without explicit permission given by the subject of the photo or video and a member of staff.
12. Pupils exhibiting harassing, intimidating behaviour or found bullying through the use of a personal electronic device are subject to discipline under the School's Anti-Bullying and Behaviour Policies.
13. Pupils are responsible for maintaining their own personal electronic devices. The School will not service, repair or otherwise maintain any technology brought to the School.
14. Pupils accessing the Internet on their personal electronic devices in school must only do so via the School's Wi-Fi network. Mobile data connections must be turned off. No other wireless, wired or internet service is permitted. The use of remote proxy services to circumvent filtering and security systems is forbidden and use of these may result in disciplinary action as appropriate.
15. Pupils keep their personal ICT device with them at all times or locked away in provided personal lockers when devices are not in use. Pupils must take full responsibility for their devices. The School will provide lockers for safe storage but the school is not responsible for the security or insurance of personal devices and they should not be left at school before or after school hours.
16. Pupils should password protect their device and remember their password. They are encouraged to personalise or label their cases as they are so many similar devices in the school.
17. Pupils must check their personal ICT device regularly to ensure the device is free from unsuitable material and viruses etc. before bringing the device into school.
18. Pupils must check their personal ICT device regularly for basic Health and Safety compliance to ensure it is free from defects. Personal ICT devices that have any Health and Safety defects should not be brought into school.
19. Remember that the School monitors use of its systems, and can view content accessed or sent via its systems.

School Liability Statement

Pupils bring their personal ICT devices to use at Stafford Grammar School at their own risk.

Pupils are expected to act responsibly with regards to their own device, keeping it up-to-date by using a fully supported operating system and via regular anti-virus and operating system updates, ensuring the device is as secure

as possible. It is their duty to be responsible for the upkeep, safety and protection of their devices. Pupils should lock their devices away in their allocated lockers when not in use.

Stafford Grammar School is in no way responsible for:

- Personal devices that are lost, stolen or broken while at school or during school activities;
- Maintenance or upkeep of any device (charging, installing updates, fixing software or hardware).

Parents should ensure that they have adequate insurance cover in place to cover the cost of repair or replacement of a personal ICT device in the event of loss/damage to the device.

Online behaviour

As a member of the school community pupils should follow these principles in all of their online activities:

- Ensure that online communications, and any content shared online, are respectful of others.
- Must not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene or promotes violence, discrimination or extremism).
- Respect the privacy of others. Must not share photos, videos, contact details or other information about members of the school community without their permission, even if the content is not shared publicly.
- Must not access or share material that infringes copyright, and must not claim the work of others as your own.
- Must not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities. Any illegal activity may be reported to the police.
- Staff must not communicate with pupils using personal email or social media accounts. Likewise, pupils must not communicate with staff using personal email or social media accounts.

Section 2 ICT Security

Guidelines for all Users of the School ICT Equipment/Network

Access to the school ICT equipment will be provided for you to carry out recognised schoolwork only, providing you abide by the following guidelines.

All pupils will be issued with a username, which will remain with them throughout their time at the school.

Any files/data stored on the School network will be treated as school property. The school may look at files and communications to ensure that the system is being used responsibly.

All actions taken on the school network are continually audited for each user.

1. Eating or Drinking is not permitted in the ICT rooms.
2. All work created by pupils should be stored in their personal folder (Drive P:) or in Google Drive. Pupils should not store work on the desktop or any other folder.
3. Important data or files should also be backed up by the student onto removal media such as Google Drive.
4. If a "Virus alert" occurs please inform a member of staff.
5. Only access school IT systems using your own username and password.
6. Do not share your username or password with anyone else. If you think that someone may know your password, change it immediately.
7. Do not attempt to access parts of the school's IT systems which you do not have permission to access, or look for vulnerabilities in the systems.
8. The unauthorised access or use of personal information, contrary to the provisions of the "Data Protection Act", is not permitted.
9. No programs should be installed or downloaded onto School computers.
10. Pupils should only print documents when they have been given permission to do so. Printing should be kept within reasonable limits. It is not acceptable to print large pieces of coursework on School printers unless you have been given express permission to do so.
11. The unauthorised copying of software, contrary to the provisions of the "Copyright, Designs & Patents Act 1988", is not permitted.
12. The installing, downloading, copying or transmitting of any content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is of a pornographic nature, obscene or promotes violence, discrimination or extremism) is forbidden.
13. Computer Equipment that belongs to the school must not be removed without formal authorisation.
14. Always ensure that you have logged off your computer before leaving it unattended.
15. Please leave the computer and the surroundings as you find them.

File/Data Security

All users have their own area for storing their work on a network server. This area is always mapped as drive P:. This means that all pupils can access their work from any terminal.

Precautions have been taken to minimise the chance of being infected by a computer virus via the Internet, email or file transfer. The school has installed its IT system with anti-virus software.

A backup of all important data is taken every night, this includes pupils' personal folders.

Guidelines for Use of the Internet and Email

Internet and Email/Gmail access will be provided for you to conduct research and to communicate with others, but only on the understanding that you agree to the following guidelines.

Stafford Grammar School conduct their own filtering services, which means that every page that is accessed or attempted to access on the Internet by users at the School can be logged. These logs will be periodically checked and any access that contradicts the below guidelines will be dealt with appropriately.

The following is NOT permitted:

1. Sending, displaying or trying to access any obscene or offensive material.
2. Harassing, insulting or attacking others through electronic media.
3. Violating Copyright laws.
4. Revealing any personal information i.e. the home address or personal phone numbers of yourself or others.
5. Downloading games or any other executables.
6. Intentionally wasting resources on unnecessary or unauthorised activities.

Check with a member of staff before:

1. Opening unidentified email attachments.
2. Completing questionnaires or subscription forms.

Section 3 Student G Suite Acceptable Use Policy

Where this policy specifically refers to G Suite it applies to all Google services accessed using your email username and password, e.g. Google Drive, Google Classroom etc.

General Principles

- Pupils must not share passwords or use another Student's account.
- Use of email by pupils is permitted and encouraged where such use is suitable for school purposes and supports the goals and objectives of the School. Users must follow this e-mail etiquette policy in sending any e-mails both internally and externally.
- School G Suite accounts are to be used for School business e.g.

contacting staff, other pupils or outside agencies related to school.
Limited personal use is considered acceptable.

- Use of G Suite may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example the Police can have a right of access to recorded data in pursuit of a crime.

Unacceptable use or behaviour:

It is unacceptable to;

- Encourage or ask for emails that are unrelated to school activities or for personal gain.
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School, or the School itself.
- Waste time on non-School related activities.

Users should:

- Keep emails brief and use meaningful subject lines.
- Re-read messages before sending to check for clarity and to make sure that they contain nothing which will make the school liable.
- Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email.
- Archive effectively - use folders and delete any messages you no longer need.
- Don't overuse the "URGENT" flag as it will lose its value.
- Never reply to spam.
- Avoid using email for sensitive or emotional messages or offensive content.
- Users should be careful when replying to emails previously sent to a group.

Monitoring

The School accepts that the use of email is an extremely valuable research and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the school's public profile. As a result;

- The School maintains the right to access user email accounts.
- Users should expect school sanctions to be used in the same way as if email content was printed out and distributed in school.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting your access to school IT systems.

If you become aware of a breach of this policy or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the Designated Safeguarding Lead (or Deputy DSL) or another member of the Senior Leadership Team.

Stafford Grammar School acknowledges an obligation to ensure appropriate security for all ICT data and equipment for which it owns and controls.