ST GABRIEL'S
NEWBURY

Including our Early Years Foundation Stage provision

Technology Use Policy and Agreement for Pupils

Date	Summer 2024 (1-0-0) Spring 2025 (1-0-1)

Purpose

The purpose of this policy is to ensure that you, as a pupil, are aware of your individual responsibilities around using technology when in school. Other policies that refer to the use of technology in school are the Anti-Bullying policy, the Child Protection (Safeguarding) Policy and Guidance and the E-Safety policy.

Scope and Definitions

This policy applies to all pupils who use or access the school's systems or information using the school's equipment or a device that is not the property of the school. This can include use of technology to support learning, the use of devices and phones, email and the internet (including AI), and the use of online tools or apps. This can include personal data as defined by the General Data Protection Regulations (2018) and the Data Protection Act (2018). The policy also includes being connected to the school's wifi network or using technology with no connection to a school network.

Roles and Responsibilities

Data Protection law says the school must ensure that it remains in control of the data for which it is responsible.

In general, the school's technology services should only be used for your study, and you must ensure that the following rules are followed:

- Your use of the school's technology services including AI must always comply with the law and school rules, whether or not you are using a device that belongs to the school.
- Respect the privacy of others. Do not take/record or share photos, videos, audio content, contact details, or other information about members of the school community without the correct permissions. Covert recording of any member of the school community is not permitted. Any improper actions in this respect may be dealt with using the school's Anti-Bullying, Behaviour, or Exclusion Removal and Review policy.
- Do 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, or raises safeguarding issues).
- Do 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.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access
- You must use passwords of appropriate length and complexity to secure your access to the school systems either on school devices or your own device. You must not disclose this password to anyone else. The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- You must lock any school or own device if it is to be left unattended.
- You must not access any program, app or data which has not been specifically authorised for your use; You must not use or copy any data or program belonging to another person without their permission.
- Do not access or share material that infringes copyright, and do not claim the work generated by AI or by other people as your own
- You must not use school technology services to be unkind to or bully another person.

- Your use of technology must be only as the teacher directs during lessons. Any other use, such as messaging others without permission, is prohibited.

Pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

It is a condition of use of the facilities that you give the School permission to check your use of the school 's technology services and devices if the Principal has reasonable suspicions that you have broken any of the rules above. Any device may be confiscated for this reason or as part of a disciplinary procedure or sanction.

Data Breach

Pupils must tell a teacher as soon as possible if they think that they or someone else has

- seen information that they should not have or
- received an email in error, or received a suspicious email
- lost their device
- deleted or copied any information that they shouldn't have.
- been asked to share data in an incorrect way

Use of MS Teams, Mail Groups or other messaging services

The school creates Teams and Groups, with pupils as members. Their use is subject to certain conditions, and these are set out below:

- **Pupils must not use technology to communicate anything offensive or unkind to others**. Ensure that your online communications, and any content you share online, are respectful of others and are written in a way you would wish to stand by. In particular, you must not send messages intended to hurt somebody else - this is a form of bullying and will be dealt with extremely severely. Nor may you send messages to other people that are offensive about someone else or contain terrorist or extremist material. Further details about cyberbullying are contained in the Anti-Bullying Policy and any concerns about communication or messages sent between pupils outside of school can be dealt with using the school's Behaviour, Anti-Bullying, or Exclusion, Removal and Review Policies.
- **Pupils should respect the privacy of others**. Do not take or share photos, audio or video recordings, contact details or other information about members of the school community using either school equipment or personal equipment, without permission from a teacher and with the consent of all parties involved. Covert recording is not permitted. Any pupil who breaks this rule can be dealt with using the school's Behaviour, Anti-Bullying, or Exclusion, Removal and Review Policies.
- Pupils should be aware that all emails sent or received on school systems will be routinely deleted after X years and your school IT account will generally be closed within 6 months of that person leaving the school.

Mobile Phone Use

In the Senior School pupils may not use mobile phones during the school day unless instructed by teachers in lessons. This includes at break or lunchtime.
If phones are brought to school, they must be kept in your device locker between 8.40am and 4.00pm, unless specific permission has been given by a Head of School or a similar member of staff.
Any use outside of these hours while you are on school premises or out of school under school supervision must abide by these technology use rules.

In the Sixth Form, pupils are allowed to use phones as a device during independent study or lessons as directed by a teacher.

Compliance with related school policies

Including our Early Years Foundation Stage provision

To the extent they are applicable to you, you will ensure that you comply with the school's E- Safety Policy and Anti-Bullying, Behaviour and Data Protection Policy.

Internet and Wifi Use – including AI facilities

Pupils' use of the Internet and wifi must always be in accordance with the law and school rules and guidelines.

As per the School's E-safety policy, monitoring and filtering software is in place to limit access to certain sites and pages, including the use of the Home Office terrorist block-list to block terrorist content as per government guidelines; all accesses to the Internet are logged and checked to fulfil the School's obligations. Staff and pupils must inform the Executive immediately of cases of misuse either accidental or otherwise. It is recognised that hits on unsuitable pages will occasionally be made by accident. However, if a deliberate pattern of use emerges then investigation may be necessary in accordance with the school's E-Safety policy.

The use of any VPN by pupils is prohibited whilst on school premises, or out of school on a school-related activity. This applies to any device or phone used by pupils.

These rules and guidelines are designed to give freedom whilst retaining a structure of legal compliance, guidance, education and courtesy to others and may be subject to change as national and international law varies or as technology advances.

In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health, medical, or wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations from a teacher.

At the start of every academic year advice and information is made available to parents on their child's use of the internet. This can be through the "Welcome To…" meetings or other communication.

Pupils are taught about internet safety, including the appropriate use of social media together with the risks of radicalisation, during PSHE lessons, in consultation with the School's own CEOP trained staff.

- The Internet and wifi system are provided for pupils and teachers to enhance educational opportunities in school. Access is a privilege, not a right, and that access requires responsibility.

- Files and communications may be reviewed to ensure that users are using the system responsibly. Teachers will monitor technology activity during lessons. Users should not expect that files stored will always remain private, and they remain the property of the School at all times.

Those who do not comply with these rules may have their access to technology and services removed or restricted or further measures may be taken as deemed necessary by the Principal, including the use of sanctions referred to in the Behaviour, or Exclusion, Removals and Review Policies.

Parents of younger children or pupils new to the school are asked to read this agreement with their child and complete this online form to confirm that their child understands and accepts this policy.

Including our Early Years Foundation Stage provision

Older pupils or existing pupils will be asked periodically to confirm their acceptance of this agreement and policy within school.

It is expected that parents will encourage their children to follow this agreement and themselves also respect the privacy and data protection of all members of the school community. Clear guidelines will be given for your own recordings of school events around consent and privacy. It is expected that any use (including yours) of your child's permitted photos, and video and audio recordings (made within the school environment or community setting) will follow best privacy and data protection practice. Covert recording is not permitted, and the school cannot view or use such recordings.

Pupils who use school devices in the School will also be asked to confirm their acceptance of the terms of Appendix 1 below.

Pupils who bring their own device into School will be asked to confirm their acceptance of the terms of Appendix 2 below.

Appendix 1 - SCHOOL OWNED DEVICES
ACCEPTABLE USE GUIDELINES

The guidelines, procedures and information in this document apply to all devices provided to pupils by the school during the prescribed time period. Teachers and other school staff may also set additional requirements for use inside and outside their classrooms.

These guidelines should be read in conjunction with the whole school Technology Use Policy. Parents are asked to read these and confirm their acceptance of these guidelines and policies.

Ownership

- The device is the property of the school and must be returned, along with the charger, protective case and any other supplied equipment, upon demand (including when a pupil leaves the school).
- The device must be returned when requested by the school, or when the pupil leaves the school or transfers to another stage of the school..

User Responsibilities (Staff, Pupils & Parents)

- Users must use the protective covers/cases provided for their device.
- The screen is made of glass and therefore is subject to cracking and breaking if misused. Never drop or place objects (books, laptops, etc.) on top of the device.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the screen.
- Do not subject the device to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph or video any other person without that person's consent and instructions from a member of staff.
- The device is subject to routine monitoring by St Gabriel's. Devices must be surrendered immediately upon request by any member of staff (with passcode).
- Users in breach of this or the Technology Use Policies may be subject to but not limited to; confiscation, removal of content, disciplinary action or referral to external agencies in the event of illegal activity.
- St Gabriel's is not responsible for the financial or other loss of any personal files that may be lost or deleted from a device.

Additional Responsibilities for Pupils

- Pupils must bring their device to school each day fully charged.
- Pupils must always keep their own photograph as their lock screen in the Junior School, as this will assist with device identification. School devices used by other pupils must be clearly named.
- Pupils must only use their device in locations permitted by staff and by school rules.
- Pupils must not use their device to send messages/emails during the school day without permission from a member of staff.
- Academic work should be stored using cloud storage (e.g. OneDrive) to ensure adequate backups are being taken. It is the responsibility of the pupil to ensure that work is being saved in the correct place. Class teachers will be able to provide guidance if needed.
- No apps installed by the school should be removed from the device.
- Photos and videos in the camera roll that are no longer needed must be deleted or removed from the device at regular intervals.
- If a pupil forgets their passcode, they must notify their form teacher as soon as possible.
- In the event of any disciplinary action, the completion of all class work remains the responsibility of the pupil.

Safeguarding and Maintaining as an Academic Tool

- The whereabouts of the device should be always known.
- It is a user's responsibility to keep their device safe and secure.
- Other users' devices are not to be tampered with.
- If a device is found unattended, it should be given to the nearest member of staff.

Mobile Device Management (MDM) Software & Monitoring

- All school devices are installed with MDM software. This software allows the school to manage the device remotely including, but not limited to:
    - Resetting the password
    - Wiping the device
    - Tracking the location of the device
    - Viewing the installed applications
    - Changing the settings
    - Monitoring information about the device.
- The device will be set up to allow location services to track and monitor the device. This setting must not be turned off.
- The MDM software and any other applications installed by the school must not be deleted.
- The school may monitor the use of the device in accordance with this Technology Use policies.

Lost, Damaged or Stolen Device

- If the device is lost, stolen, or damaged, the school IT manager or a senior member of staff must be notified immediately.
- Devices that are believed to be stolen can be tracked through our MDM software.
- Devices which are stolen (a police report will be required) or accidentally damaged will be replaced/repaired by the school provided reasonable steps have been taken to protect the device and the school's policies and guidelines have been adhered to. Parents will be responsible for replacing lost devices.

Prohibited Uses (not exhaustive)

- Accessing Inappropriate Materials. All material on the device must adhere to the Technology Use policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening or inappropriate materials.
- Illegal Activities. Use of the school's resources (e.g. software or devices) for financial or commercial gain or for any illegal activity is not allowed.
- All users must follow the school rules and abide by the rules and responsibilities given in this policy and the E-safety policy, including those about the use of AI.
- Cameras. As above, images or video can only be taken under instruction from a teacher and with the consent of the subject. The user agrees that the camera will not be used to take inappropriate or illicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of the camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation of these guidelines and is a disciplinary offence. Use of the camera and microphone to record a teacher is strictly prohibited unless permission is granted by that teacher. Again, this will be treated as a serious violation of these guidelines and is a disciplinary offence.
- Posting school content or images or video of others on the Internet (e.g. social media or chat groups etc.) is strictly forbidden, without the express permission of the teacher or, in the case of staff use, a member of the Senior Leadership Team. Further information about preventing cyber-bullying is contained in our Anti-Bullying Policy and our Technology Use Policy.
- Misuse of Passwords, Codes or Other Unauthorised Access. Pupils must use their passcode on their device to prevent other users from misusing it. They should keep this secret and must not attempt to change it without permission from a member of staff.
- Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.
- Malicious Use/Vandalism. Any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- Users should also be aware of and abide by the guidelines set out by the school's Technology Use Policy which is available on our website.
- St Gabriel's reserves the right to confiscate and search a device to ensure compliance with these guidelines.

Revisions

- These guidelines may be updated from time to time. Parents will be advised of any amendments and will be expected to discuss these with their child.

Parents are asked to confirm that they understand these guidelines and have explained them to their child. A pupil friendly version is given below for Junior School Pupils.

JUNIOR PUPIL PLEDGE FOR DEVICE USE

I will take good care of my device and I will never leave the device unattended.

I will always have my photo set as my screen-lock picture.

I will never lend my device to others.

I will know where my device is at all times.

I will charge my device's battery every night.

I will keep food and drinks away from my device since they may cause damage.

I will not disassemble any part of my device or attempt any repairs.

I will protect my device by leaving it in the case at all times.

I will not use my device to send messages/emails during the school day without permission.

I will use my device in ways that are appropriate.

I understand that my device is subject to inspection at any time without notice.

I will only photograph or video people with their permission.

I will only use the camera or the microphone when my teacher tells me to.

I will never share any images or movies of people on the internet, unless I am asked to do so by my teacher.

I will tell my form teacher straight away if I forget my passcode

Appendix 2 – PUPILS' OWN DEVICES
ACCEPTABLE USE GUIDELINES

Pupil Responsibilities

- The device may be subject to routine monitoring by St Gabriel's. Devices must be surrendered immediately upon request by any member of staff (with passcode).
- Users in breach of this or the Technology Use Policies may be subject to but not limited to; confiscation, removal of content, disciplinary action or referral to external agencies in the event of illegal activity.
- St Gabriel's is not responsible for the financial or other loss of any personal files that may be lost or deleted from a device.
- Pupils must bring their device to school each day fully charged.
- Pupils must not use their device to send messages/emails during the school day without permission from a member of staff.
- Academic work should be stored using cloud storage (e.g. OneDrive) to ensure adequate backups are being taken. It is the responsibility of the pupil to ensure that work is being saved in the correct place. Class teachers will be able to provide guidance if needed.
- In the event of any disciplinary action, the completion of all class work remains the responsibility of the pupil.
- Pupils must be able to access websites and apps as required by teachers. Parental acceptance of these terms implies pupils may use websites or apps that require parental consent when directed to do so by a member of staff.

Safeguarding and Maintaining as an Academic Tool

- The whereabouts of the device should be always known.
- It is a user's responsibility to keep their device safe and secure.
- Other users' devices are not to be tampered with.
- If a device is found unattended, it should be given to the nearest member of staff.

Prohibited Uses (not exhaustive)

- Accessing Inappropriate Materials. All material on the device must adhere to the Technology Use policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening or inappropriate materials.
- Illegal Activities. Use of the school's resources (e.g. software or devices) for financial or commercial gain or for any illegal activity is not allowed.
- All users must follow the school rules and abide by the rules and responsibilities given in this policy and the E-safety policy, including those about the use of AI.
- Cameras. As above, images or video can only be taken under instruction from a teacher and with the consent of the subject. The user agrees that the camera will not be used to take inappropriate or illicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of the camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation of these guidelines and is a disciplinary offence. Use of the camera and microphone to record a teacher is strictly prohibited unless permission is granted by that teacher. Again, this will be treated as a serious violation of these guidelines and is a disciplinary offence.
- Posting school content or images or video of others on the Internet (e.g. social media or chat groups etc.) is strictly forbidden, without the express permission of the teacher or, in the case of staff use, a member of the Senior Leadership Team. Further information about preventing cyber-bullying is contained in our Anti-Bullying Policy and our Technology Use Policy.
- Misuse of Passwords, Codes or Other Unauthorised Access. Pupils must use their passcode on their device to prevent other users from misusing it. They should keep this secret and must not attempt to change it without permission from a member of staff.
- Any user trying to gain access to another user's accounts, files or data will be subject to disciplinary action.
- Malicious Use/Vandalism. Any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- Users should also be aware of and abide by the guidelines set out by the school's Technology Use Policy which is available on our website.

- St Gabriel's reserves the right to confiscate and search a device to ensure compliance with these guidelines.

Revisions

- These guidelines may be updated from time to time. Parents will be advised of any amendments and will be expected to discuss these with their child.

Parents are asked to confirm that they understand these guidelines and have explained them to their child if necessary.

Date	**Change History**
Summer 2024 1-0-0	Policy written – replacing ICT Acceptable Use Policy for pupils
Sprint 2025 1-0-1	Updates for AI