



**BEDFORD  
GIRLS  
SCHOOL**

Reviewed May 2025

Next review date August 2026

Reviewed by: Director for Digital Learning, Enterprise, and Sustainability

# Technology for Learning - Acceptable Use Policy

## Introduction

The focus of Technology for Learning and the 1:1 iPad initiative at Bedford Girls' School is to provide tools and resources for the 21<sup>st</sup> Century Learner.

Excellence in education requires that technology is seamlessly integrated throughout the educational programme. Increasing access to technology is essential for that future, and one of the learning tools for these 21<sup>st</sup> Century students is the tablet computer.

The individual use of iPad devices is a way to empower students to maximise their full potential and to prepare them for university and the workplace. We believe that learning results from the continuous dynamic interaction among students, educators, parents and the extended community.

The policies, procedures and information within this document apply to all devices, applications and digital tools used at Bedford Girls' School, including any other device considered by the school to come under this policy. Teachers may set additional requirements for use in their classroom.

## Acceptable Use

### *Overview*

This document outlines the shared responsibility of use of technologies and networks provided by Bedford Girls' School.

Bedford Girls' School recognises that access to technology in school gives students and teachers a greater opportunity to learn, engage, communicate and develop skills that will prepare them for work, life and citizenship. We are committed to helping students develop 21<sup>st</sup> Century technology and communication skills.

To that end, we provide access to technologies for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviours that students are expected to follow when using school technologies or when using personally owned devices in the school grounds.

### **Technologies Covered**

Bedford Girls' School provides a range of technological facilities and services hosted both by the school and by other organisations.

As new, suitable technologies emerge, Bedford Girls' School may provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

## General Guidance

All technology access provided by BGS is intended for educational purposes. All digital citizens are expected to use good judgment and to follow the spirit of this document as well as the specifics of it: they should be safe, appropriate, careful and kind; they should not try to defeat or circumvent technological protection measures, but use good common sense and seek guidance where they are unsure what action to take.

**Digital Citizenship** is a concept which helps teachers, technology leaders and parents to understand what students should know in order to use technology appropriately. **It is the responsibility of all members of the school community.** Digital Citizenship is more than just a teaching tool; it is a way to prepare students for a society in which technology is ubiquitous.

Digital Citizenship is a framework representing the accepted standards of appropriate and responsible technology use. The issue is more than what the students do or do not know, but what is considered appropriate use of technology. The Digital Citizenship programme at Bedford Girls' School focuses on the seven elements of being a responsible digital citizen. A brief description of these can be found below:

### 1. Digital Commerce

Electronic buying and selling of goods. Have the appropriate care and precautions been taken to buy and sell successfully in a digital world?

### 2. Digital Literacy

The capability to use digital technology and the knowledge of when and how to use it. Have our digital citizens taken the time to learn about digital technologies? Do they share that knowledge with others?

### 3. Digital Etiquette

The standards of conduct expected by other digital technology students. Do students consider others when using digital technology? Do they know how to respond appropriately in a given situation?

### 4. Digital Law

The legal rights and restrictions governing technology use. Are students aware of laws (rules, policies) that govern the use of digital technologies? Are they aware of the legal implications?

### 5. Digital Rights and Responsibilities

The privileges and freedoms extended to all digital technology students and the behavioral expectations that come with them. Are students ready to protect their digital rights and digital rights of others?

### 6. Digital Health and Wellness

The elements of physical and psychological well-being related to digital technology use. Do students consider the risks (both physical and psychological) when using digital technologies?

### 7. Digital Security

The precautions that all technology students must take to guarantee the personal safety and security themselves and others. Do students take the time to protect their information while creating precautions to protect others' data as well?

## Limitation of Liability

BGS will not be responsible for damage or harm to persons, files, data or hardware. While BGS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. BGS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

## **Violations of this Acceptable Use Policy**

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology or computer privileges in extreme cases.
- Notification to parents in most cases.
- Detention or suspension from school and school-related activities.

## *Use of the School Network*

The school network is intended for educational purposes. All activity over the network will be monitored (both over the wired network and wifi).

All use of the school network shall be via individually authorised school network account. Users may not share their network account access with others. Gaining access to another student's accounts, files and/or data is strictly forbidden.

The following activities are strictly forbidden: participation in credit-card fraud, electronic forgery or other forms of illegal behaviour; vandalism (any malicious attempt to harm or destroy hardware, software or data, including but not limited to the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment; Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients; bypassing the school's security; accessing a device remotely without express permission.

## *Prohibition of VPN Usage*

Bedford Girls' School strictly prohibits the use of Virtual Private Networks (VPNs) in school to facilitate proxy avoidance by students and staff. VPNs bypass the school's filtering and monitoring systems, undermining safeguarding measures designed to protect students from harmful online content and cyber threats.

The school's firewall actively detects and blocks VPN usage. Any attempt to access the internet through a VPN or proxy service is considered a direct violation of our digital safety policies.

## **Example Scenarios:**

- A student attempts to access a restricted website by using a VPN app or website on their device—this is prohibited.
- A staff member uses a VPN to bypass content filters—this is a breach of school policy.

All users of the school's network must comply with the filtering and monitoring guidelines in place to ensure a safe digital environment.

## *Access to the Internet from the School Network*

BGS provides its students with access to the Internet, including websites, resources, content and online tools in compliance with school policy.

Access to the Internet will be restricted by our firewall in accordance with policies and regulations, such as the Keeping Children Safe In Education (KCSIE 2024). Users are expected to respect web filtering as a safety precaution and should not try to circumvent it when using the Internet. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to notify IT Support via the Helpdesk to request access.

For the security of our network, users should download such files only from reputable sites, and only for educational purposes. Peer-to-peer downloading is considered very high-risk and is not permitted from the school network.

Web browsing is monitored and activity records may be retained indefinitely.

Use of any information obtained via BGS's designated Internet system is at your own risk.

Students are expected to follow the school rules and demonstrate the good conduct outlined later in the policy

The following activities are strictly prohibited and will be treated as gross misconduct:

- Viewing, accessing, or downloading pornographic, terrorist, extremist, or any other material that the School deems inappropriate or unsuitable.
- Sending, receiving, uploading, downloading, or distributing materials that are offensive, profane, threatening, pornographic, obscene, or sexually explicit.
- Engaging in plagiarism, including accessing websites that sell examination papers, book reports, or other forms of student work.

Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the School.

### *Email*

BGS provides students and staff with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

Email accounts should be used with care. Students should only communicate with others as allowed by the school. Students should not send personal information by email. Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Users should not attempt to open files or follow links from unknown or untrusted origin; Users should use appropriate language; and demonstrate good conduct outlined later in the policy

The following activities are strictly prohibited:

- Sending spam, including mass emails or inappropriate messages.
- Using school email accounts for financial or commercial purposes.
- Using school email accounts for any illegal activities.

### *Mobile Devices*

BGS may provide students with laptop computers or other devices to promote learning both inside and outside the classroom.

Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Installing unapproved or unlicensed apps, accessing VPNs, games, content or programs is strictly forbidden.

Users are expected to treat these devices with due care and caution; these are expensive devices that the school is entrusting to their care. Users agree to use devices in an appropriate manner so as not to damage school equipment. This "damage" includes, but is not limited to, the loss of data resulting from delays, non-deliveries or service interruptions caused by the student's own negligence, errors or omissions.

Students should report any loss, damage, or malfunction to IT Support staff immediately. iPad devices are insured but students may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices, including the use of the school network, may be monitored.

### *Personally-owned Devices (BYOD)*

Years 7–10

To maintain a safe, secure, and educationally focused digital environment, students in Years 7 to 10 are expected to use only their school-issued iPad while on school premises and adhere to the following regulations:

- Years 7-10 are permitted to use their school iPad only, and must ensure their mobile phone is secured in their phone pouch at the appropriate times.
- Year 11 are permitted to use their school iPad only, and must ensure mobiles are used only in the Common Room between 8.40 and 16.00

Years 7-11 are not permitted to use their own tablets and laptops in school. Failure to comply with these instructions will result in disciplinary action as outlined within the school Behaviour Policy.

- 6th Form students are permitted to use their own devices in school but must abide by the Acceptable Use, Safeguarding and Filtering and Monitoring policies when accessing the school network

The use of any personal device (including tablets, laptops, or smartphones as per the year group restrictions) that is capable of independently connecting to the internet via mobile data (e.g., SIM cards, hotspots, tethering) is not permitted during the school day.

Personal devices that bypass the school's network controls constitute a form of proxy avoidance, preventing the school from fulfilling its legal safeguarding obligations, including the ability to monitor online activity and filter harmful or inappropriate content. As such, this represents a serious breach of our digital safety protocols.

Personal devices are not supported by IT Support or covered by the school's insurance policy. Any misuse of personally-owned devices may result in disciplinary action. Where applicable the use of personal devices is covered by the same conduct, acceptable use policies and guidelines as school-provided equipment.

Use or possession of hacking software is strictly forbidden.

### *Network and Device Security*

Users are expected to take reasonable precautions against the transmission of malware over the school network. This includes not knowingly opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If users believe a computer or mobile device they are using has been compromised, they should alert IT Support immediately. Users of school devices should not attempt to remove the virus themselves or download any programs to help remove the virus.

### *Artificial Intelligence*

As a school we embrace the positive use of AI to enhance human productivity. We also strongly promote its ethical and moral use.

Any use of AI technologies to cause harm or breach existing rules or elements of the Acceptable Use policy, Safeguarding or Positive Behaviour policies would be viewed as prohibited and the responsibility of the user.

Further guidance about the use of AI for school work is held in the Academic Honesty policy.

### *Copyright and Plagiarism*

Students should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet or using AI tools and Large Language Models (LLMs) such as ChatGPT. Students should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online. Research conducted via the internet should be appropriately cited, giving credit to the original author. Students should be aware of the Academic Honesty Policy where this is outlined in more detail.

### *Collaborative Tools*

Recognising that collaboration is essential to education, BGS may provide students with access to websites or tools that allow communication, collaboration, sharing and messaging among students.

Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing and messaging may be monitored. Students should be careful not to share personally identifying information through these tools.

### *Conduct*

Users should always use the Internet, network resources and online sites in a courteous and respectful manner.

Students should recognise that content on the Internet is not necessarily correct, appropriate or verifiable. Students should maintain an awareness of the reputation of the source when conducting research via the Internet.

### **The Sharing of Information**

Students should remember not to post anything online that they wouldn't want parents, teachers or future colleges or employers to see. Once something is online, it's out there – and can sometimes be shared and spread in ways that were never intended.

Students should never share personal information, including phone number, address, birthday, or financial information over the Internet without appropriate adult permission.

### **Personal Safety**

Students should recognise that communicating over the Internet does not bring anonymity and can result in associated risks, and should carefully safeguard the personal information of themselves and others.

Students should never agree to meet someone they have contacted online in real life without parental permission.

If students see a message, comment, image, or anything else online that makes them concerned for their personal safety, they should bring it to the attention of an adult (teacher or staff if at school; parent if using the device at home) immediately.

### **Cyberbullying**

Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, tricking, excluding and cyberstalking are all examples of cyber-bullying. Students should not be mean. Students should not send emails or post comments with the intent of scaring, insulting, hurting or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges as outlined in the Antibullying Policy. In some cases, cyberbullying can be a criminal offense.

## *Responsible Use of Photos and Videos*

As part of Bedford Girls' School's commitment to safeguarding, student privacy, and upholding a respectful school environment, students must adhere to the following guidelines regarding photography, videography, and recordings.

- **Consent & Privacy:** Students must not take photos or record videos of other students, staff, or visitors without explicit consent.
- **Appropriate Use:** Photos and videos taken for educational purposes must be stored securely and used only within the context of school-related activities. Any media containing other students must not be shared without permission.
- **Prohibition on Recording Lessons & Staff:** Students are strictly prohibited from recording lessons, teachers, or staff members without prior approval from the school. Unauthorised recordings undermine a safe learning environment and violate privacy expectations.
- **Social Media & Online Sharing:** Students must not post or share any photos or videos taken at school on social media, messaging apps, or any online platform without explicit approval from a teacher.
- **Safeguarding & GDPR Compliance:** Any misuse of photos or recordings, including the unauthorised sharing of images or videos that could result in bullying, harassment, or data breaches, will be treated as a safeguarding issue. This includes the manipulation of images or data and augmenting technologies that breach our expectations.

### **Example Scenarios:**

- A student records a teacher's lesson and shares it online—this is strictly prohibited.
- A student takes a photo of a classmate without asking and sends it in a group chat—this is a violation of privacy and school policy.
- A student takes a picture of their science project to submit for homework—this is acceptable.
- A student creates a video project during a lesson with permission from the teacher - this is acceptable

## *Examples of Acceptable Use*

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognise that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. students should use their own good judgement when using school technologies.

## *Examples of Unacceptable Use*

I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment or disrespectful conduct toward others – staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Send spam or chain mail.
- Plagiarize content I find online.
- Post personally-identifying information about myself or others.
- Agree to meet someone I have contact with online in real life without parental permission.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to circumvent or access sites, servers, accounts, or content that isn't intended for my use.

This is not intended to be an exhaustive list. students should use their own good judgement when using school technologies.



# Social Media

This document outlines the shared responsibility of use regarding Social Media.

We encourage teachers, students, staff and other school community members to use social networking/media as a way to connect with others, share educational resources, create and curate educational content, and enhance the classroom experience. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.

We've created these social networking/media guidelines for you to follow when representing the school in the virtual world.

Please do the following:

## *Use good judgment*

We expect you to use good judgement in all situations.

You must know and follow the school's Acceptable Use Policy.

Regardless of your privacy setting, assume that all of the information you have shared on your social network is public information.

## *Be respectful*

Always treat others in a respectful, positive and considerate manner.

## *Be responsible and ethical*

Even though you are approved to represent the school, unless you are specifically authorised to speak on behalf of the school as a spokesperson, you should state that the views expressed in your posting, etc. are your own. Stick with discussing school-related matters that are within your area of responsibility.

Be open about your affiliation with the school and the role/position you hold.

## *Be a good listener*

Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly and share feedback.

Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback, etc. Always do as much listening and responding as you do "talking".

## *Don't share the following:*

### **Confidential information**

Do not publish, post or release information that is considered confidential. If it seems confidential, it probably is. Online "conversations" are never private. Do not use your birth date, address or mobile phone number on any public website.

## **Private and personal information**

To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.

Never give out or transmit personal information of students, parents or members of staff. Don't take information you may receive through social networking (such as email addresses, customer names or telephone numbers) and assume it's the most up-to-date or correct.

Always respect the privacy of the school community members.

## **Images**

Respect brand, trademark, copyright information and/or images of the school (if applicable). You may use photos and video (products, etc.) that are available on the school's website. It is not acceptable for students to post pictures without the express consent of the individual.

Do not post pictures of others without their permission.

## **Other sites**

A significant part of the interaction on blogs, Twitter, Facebook and other social networks involves passing on interesting content or linking to helpful resources. Don't blindly repost a link without looking at the content first. Pay attention to the security warnings. They actually serve a purpose and protect you and the school.

When using Twitter, Facebook and other tools, be sure to follow their printed terms and conditions.

## *And if you don't get it right...*

Be sure to correct any mistakes you make immediately, and make it clear what you've done to fix it.

Apologise for the mistake if the situation warrants it.

If it's a **major** mistake (e.g. exposing private information or reporting confidential information) please let someone know immediately so the school can take the proper steps to help minimize the impact it may have.

## **Use of Technology**

The use of BGS's current technology resources is a privilege, not a right. The privilege of using the technology resources provided by BGS is not transferable or extendable by students to people or groups outside the school, and terminates when a student is no longer enrolled at BGS. This policy is provided to make all students aware of the responsibilities associated with efficient, ethical and lawful use of technology resources.

If a person violates any of the Acceptable Use guidelines detailed in this policy, privileges may be terminated, access to the school's technology resources may be denied and the appropriate disciplinary action will be taken. Violations may result in disciplinary action up to and including suspension/expulsion for students. When applicable, the local police force may be involved.

## *Parent/Guardian Responsibilities*

- Talk to your children about values and the standards that they should follow on the use of the internet, just as you do on the use of all media information sources such as television, telephones, movies and radio.
- Parents are to monitor the use of the iPad and Internet when students are at home.

### *School Responsibilities are to:*

- Provide internet and email access to students.
- Provide Internet blocking of inappropriate materials. We will provide staff guidance to aid students in doing research and help ensure student compliance with the Acceptable Use Policy.

### *Students are responsible for:*

- Letting IT Support know if their iPad is not working.
- Using computers/devices in a responsible and ethical manner.
- Obeying general school rules concerning behaviour and communication that apply to iPad/computer use.
- Using all technology resources in an appropriate manner so as not to damage school equipment.

This “damage” includes, but is not limited to, the loss of data resulting from delays, non-deliveries or service interruptions caused by the student’s own negligence, errors or omissions. Use of any information obtained via BGS’s designated Internet system is at your own risk. BGS specifically denies any responsibility for the accuracy or quality of information obtained through its services.

- Helping BGS protect our computer system/device by contacting IT Support about any security problems they may encounter.
- Monitoring activity on their account(s).
- Turning off and securing their iPad after they have finished working to protect their work and information.

### *Student Activities Strictly Prohibited:*

- Illegal acquisition or distribution of copyrighted materials
- Any action that violates the Acceptable Use Policy or public law.
- Sending, accessing, uploading, downloading or distributing offensive, profane, threatening, pornographic, obscene or sexually-explicit materials, plagiarism, including accessing sites selling examination papers, book reports and other forms of student work.
- Installing unapproved or unlicensed apps, games, content or programs.
- Spamming – sending mass or inappropriate emails.
- Gaining access to another student’s accounts, files and/or data.
- Use of the school’s internet/email accounts for financial or commercial gain or for any illegal activity.
- Use of anonymous and/or false communications.
- Use or possession of hacking software.
- Participation in credit-card fraud, electronic forgery or other forms of illegal behaviour.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including but not limited to the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment.
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.
- Bypassing the school’s security.
- Accessing a device remotely without express permission.

# Bedford Girls' School Student Pledge for iPad Use

*Print this page, read, sign and return to your form tutor.*

1. I will take good care of my iPad.
2. I will never leave the iPad unattended.
3. I will only use my own password and not share it with others.
4. I will never loan out my iPad to others.
5. I will ensure my iPad's battery is fully charged for the start of the school day.
6. I will keep food and beverages away from my iPad since they may cause damage to the device.
7. I will not disassemble any part of my iPad or attempt any repairs.
8. I will protect my iPad by handling it appropriately.
9. I will use my iPad in ways that are appropriate, meet school expectations and are educational.
10. I will not place decorations (such as stickers, markers, etc.) on the iPad, only on a cover.
11. I understand that my iPad is subject to inspection at any time without notice, and remains the property of Bedford Girls' School.
12. I will follow the policies outlined in the *Technology for Learning Acceptable Use Policy* while at school, as well as outside the school.
13. In case of damage I will report this to the school and to my parents immediately.
14. In case of theft I will report this to the school and to my parents immediately.
15. I will be responsible for all damage or loss caused by neglect or abuse.
16. I agree to maintain the iPad, cover and power cord in good working condition.
17. I will ensure that my device has the approved cover that will protect the device while it is in my use.
18. I will contact IT Support as soon as I identify a problem with my iPad that affects my school work.

**I have read the Bedford Girls' School Technology for Learning Acceptable Use Policy as well as the iPad Pledge. I understand and accept these conditions:**

Student Name:

Student Signature:

Date:

# Bedford Girls' School Junior School Student Pledge for iPad Use

*Print this page, read, sign and return to your class teacher.*

1. I will take good care of my iPad.
2. I will never leave my iPad unattended.
3. I will only use my own password and not share it with others.
4. I will never lend my iPad to others.
5. I will replace my iPad every day into the secure iPad locker in my classroom.
6. I will keep food and drinks away from my iPad since they may cause damage to the device.
7. I will use my iPad in ways that my teacher has asked me to and only to help me learn.
8. I will not put decorations or stickers on my iPad, only on a cover.
9. If my iPad is damaged I will tell my class teacher immediately.
10. I will take responsibility for any damage to my iPad or if I lose it because I have not looked after it carefully.
11. I will protect my iPad by handling it appropriately.
12. I will follow the policies outlined in the Technology for Learning Acceptable Use Policy while at school, as well as outside the school.

**I have read the Bedford Girls' School Technology for Learning Acceptable Use Policy as well as the iPad Pledge. I understand and agree to follow both:**

Student Name:

Student Signature:

Date: