



**Inspiring Futures
through Learning**

Inspiring Futures through Learning

**Digital Technology
Acceptable and Responsible Use Policy**

September 2026 to September 2027



Policy name:	Digital Technology Acceptable and Responsible Use Policy
Version:	V4
Date relevant from:	September 2026
Date to be reviewed:	September 2027
Role of reviewer:	Head of Information Technology and Head of System Leadership
Statutory (Y/N):	Y
Published on website*:	1A

Policy level**:	1
Relevant to:	Everyone associated with IFtL schools and departments
Bodies consulted:	Trustees
Approved by:	IFtL Board of Trustees
Approval date:	14/8/2026

Key:

* **Publication on website:**

IFtL website		School website	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

** **Policy level:**

1. Trust wide:
 - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
 - o *Approved by the IFtL Board of Trustees.*
2. Trust core values:
 - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore form the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
 - o *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
 - o *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*
3. School / department policies
 - These are defined independently by schools / departments as appropriate
 - o *Approved by school / department governance bodies.*



Digital Technology Acceptable and Responsible Use Policy

The policies, procedures and information within this document applies to all digital devices used by pupils in school. This policy must be interpreted alongside the IFtL Online Safety Policy and the IFtL Use of Artificial Intelligence Policy. Teachers and other school staff may also set additional requirements for use within their classroom, provided these do not remove, weaken or contradict the expectations in this policy.

This Acceptable and Responsible Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the users and systems at risk.

This Trust-wide policy should be used as written with staff, parents and carers. Schools must use this policy to support the creation of an age-appropriate Code of Conduct or iPad Promise for pupils. These school-level agreements should reflect the age, stage of development, context and community of the school, and should help pupils understand how to use technology positively, safely and responsibly. They should be both proactive and responsive: supporting safe and effective digital learning while also making clear the boundaries, reporting routes and responses when concerns or misuse arise. School-level agreements may be reviewed and updated during the year to respond to emerging technologies, online safety risks, safeguarding requirements, pupil voice and local context. The core expectations, safeguarding requirements and prohibited uses in this Trust-wide policy must not be removed, weakened or contradicted.

User responsibilities

- Users must use protective covers/cases for their iPad/laptop.
- Always have a passcode set on the iPad/laptop and do not share this with others.
- Users must not enter personal, confidential, sensitive or identifying information about themselves or others into unapproved websites, apps, platforms or AI tools.
- The iPad/laptop screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop nor place heavy objects (books, laptops, etc.) on top of them.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad/laptop screen.
- Do not subject the iPad/laptop to extreme heat or cold.
- Do not store or leave unattended in vehicles overnight. If the device is left in a vehicle for any short period of time, it must be turned off and stored out of sight and in the boot.
- Users may not photograph, film, record, edit, manipulate, store, forward, publish or use the image, voice or likeness of another person without explicit permission and in line with school expectations.
- The iPad/laptop, school network and Trust digital services may be filtered, monitored and reviewed by the school and Trust for safeguarding, cyber security and compliance purposes, including when devices are used off site where applicable. Devices must be surrendered immediately upon request by any member of staff.
- Users in breach of the Acceptable and Responsible Use Policy may be subject to, but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.



- When using Wi-Fi outside of school or home, make sure you are connecting to a secure network and your passcode is kept private.
- The school is not responsible for the financial or other losses from any personal files that may be deleted from an iPad/laptop or school-provided online storage. Reasonable precautions have been taken to prevent the loss of academic content/work by asking students to upload their work to Showbie (the online digital workbook) that utilises cloud storage to keep it safe and secure.
- Only charge the iPad/laptop using the plug and cable provided, ask if you need help.

Safeguarding and maintenance

- iPad/laptop batteries are required to be charged and be ready to use in school.
- Syncing the iPad to iTunes or iCloud will be managed by the Central Trust IT team.
- Items deleted from the iPad/laptop cannot be recovered.
- Memory space is limited. Devices should only be used to store academic content and the number of photographs and films should be limited. Users should be taught how to catalogue, file and delete photographs and ensure camera roll is kept a reasonable size at all times to prevent over-filling the memory of the device. All images on adult devices must be moved to an appropriate Sharepoint folder and deleted in line with retention policies.
- The whereabouts of the iPad/laptop should be known at all times.
- It is a user's responsibility to keep their iPad/laptop safe and secure.
- iPads/laptops belonging to other users are not to be tampered with in any manner.
- If an iPad/laptop is found unattended, it should be given to the nearest member of staff.
- Users must report anything worrying, unsafe, inappropriate, harmful or suspicious immediately to a trusted adult, the Designated Safeguarding Lead, Head Teacher or IFtL IT Team, as appropriate.

Lost, Damaged, or Stolen iPads/Laptops

- If the iPad/laptop is lost, stolen, or damaged, the Head Teacher and Trust IT team must be notified immediately.
- Where the iPad/laptop is believed to have been stolen, the incident should be reported to the police and a crime reference number should be obtained within 24 hours.
- If the iPad/laptop is believed to have been lost or stolen, reasonable steps should be taken to find it including, but not limited to, tracking of the device through the relevant features.
- Follow the steps referenced in the 'Home/School Agreement'.

Prohibited Uses (Not an exhaustive list)

- Accessing Inappropriate Materials – All material on the iPad/laptop must adhere to the Acceptable and Responsible Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Users must not create, ask for, view, save, send or share anything harmful, abusive, discriminatory, bullying, humiliating, nude, semi-nude, sexualised, pornographic or inappropriate, including content made or changed using Artificial Intelligence or other digital tools.
- Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.



- Violating Copyright and Intellectual Property – Users must not copy, download, use or share digital content, including text, images, music, video or AI-generated content, unless they have permission or it is allowed for educational use. Users should acknowledge sources where appropriate.
- Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit, or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of cameras in toilets or changing rooms, regardless of intent, will be treated as a serious violation.
- Images of other people may only be made with the explicit permission of those in the photograph.
- Posting of images/movies on the Internet or into any public forum is strictly forbidden, without the express permission of the Teacher or, in the case of staff use; a member of the Senior Leadership team.
- Users must not create, request, possess, share or distribute AI-generated or digitally manipulated images, audio or video of another person without permission. Any nude, semi-nude, sexualised, abusive or humiliating AI-generated or digitally manipulated content will be treated as a serious safeguarding concern.
- Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.
- Misuse of Passwords, Codes, Apple Classroom or other Unauthorised tampering: Users are required to set a passcode/password on their iPad/laptop to prevent other users from misusing it. Users must not deliberately take actions to disconnect their device from features such as Apple Classroom.
- 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.
- Jailbreaking – Jailbreaking is a process which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
- 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 must follow the expectations set out in relevant policies including, but not limited to, this policy, the IFtL Online Safety Policy and the IFtL Use of Artificial Intelligence Policy.
- Users must not attempt to bypass the set-up, filtering, monitoring or security of the device, school network or Trust systems in order to access prohibited, unknown or inappropriate material. This includes, but is not limited to, using mobile data, VPNs, proxy sites, private browsing, personal hotspots, alternative networks or any other method to avoid school or Trust controls. Any attempts to do this will be taken seriously and users may be subject to a disciplinary procedure.
- Users must only use school-approved digital tools, including AI tools, that are age-appropriate, authorised and verified by the school. Pupils must not use generative AI tools unless this has been explicitly authorised by the school for a specific curriculum purpose. AI-generated content must not be assumed to be accurate, safe, appropriate or unbiased.
- Users must not use AI or digital tools to impersonate others, create deepfakes, generate misleading information, bully, harass, coerce, embarrass or cause harm to another person.



Users should be aware that some AI tools, including chatbot-style tools, may produce inaccurate, inappropriate or misleading responses and must be used only where approved by the school.

- Private browsing must not be used to avoid school or Trust filtering, monitoring or safeguarding controls.

The school, and IFtL, reserves the right to confiscate and search an iPad/laptop to ensure compliance with this Acceptable Use Policy.

I understand that my use of technology, online services and AI must be safe, respectful, responsible, lawful and in line with school and Trust policies.

I understand that I am responsible for my actions, both in and out of school:

- The school also has the right to act against me if I am involved in incidents of inappropriate behaviours, that are covered in this agreement and other policies, whether I am in or out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- If I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities, involvement of the police.

