The Radclyffe School

"Working Together for Excellence"

STUDENT ICT ACCEPTABLE USE POLICY

Approved By	Local Governing Committee
Date Approved	Summer 2026
Review Date	Summer 2027

Contents

1. Policy Statement 1
2. Rules for ICT Use 1
    You must not: 1
    You must: 1
3. Mobile Devices 2
4. Online Safety and Digital Citizenship 2
5. Sanctions 2
6. Related Policies 2

1. Policy Statement

ICT (Information and Communication Technology) is an essential part of learning at The Radclyffe School. Students are expected to use it responsibly, safely, and respectfully. The same behaviour expectations that apply elsewhere in school also apply to ICT use.

ICT access is provided for **educational purposes only** (research, learning, and communication). It is a **privilege, not a right**, and comes with responsibilities. Parent/carer permission is required before students can use the Internet at school.

- Students are responsible for their own actions, communications, and content online.
- All activity on school systems is monitored. Authorised staff, including IT staff, may view files, emails, and internet activity **where necessary** to protect students, staff, and the school.
- Do not store sensitive or confidential information (such as passwords, medical details, or private personal data) on the school network unless instructed by a member of staff.
- The school provides filtering and firewall protection, but families are responsible for online safety outside school.

Cyberbullying, harassment, or discrimination of any kind will not be tolerated. Serious incidents may involve the **Anti-Bullying Policy**, **Safeguarding Policy**, and external authorities.

2. Rules for ICT Use

You must not:

- Send, access, create, or display offensive, abusive, or inappropriate material.
- Attempt to log in using another person's account or share your login details.
- Damage, interfere with, or bypass the school's ICT security systems.
- Copy or use material in ways that break copyright or licensing laws.
- Use AI or other online tools to generate harmful, offensive, or misleading content, or in ways that breach assessment rules or teacher instructions.
- Download, install, or run software or apps without permission.
- Use anonymous messaging, online chat rooms, or chain letters.
- Connect personal devices (phones, tablets, laptops) to the school network without authorisation.
- Use ICT for private business, financial gain, gambling, political purposes, or advertising.
- Download or stream large files that may slow down the system.
- Cheat in exams or assessments, plagiarise, or submit others' work as your own.
- Record or share images, video, or audio of staff or students without permission.
- Create, share, or use fake images, videos, audio, or profiles (including AI-generated or altered content) to impersonate or mislead others.

You must:

- Keep your password secure and never share it.
- Keep your files and work area organised; delete items no longer needed.
- Only use school-approved accounts on school devices unless a member of staff has given permission.
- Communicate respectfully online at all times.
- Respect privacy and never share personal information without permission.
- Acknowledge sources when using text, images, or data found online.

- Report anything online that makes you feel uncomfortable, unsafe, or worried to a teacher, Year Manager or the Designated Safeguarding Lead.
- Report online safety concerns even if you are unsure, worried about consequences, or think you may have made a mistake. You will be supported.
- Use social media responsibly; avoid posting or sharing anything that could harm the reputation, safety, or wellbeing of the school, staff, or students.
- Follow teacher instructions when using AI or digital tools in lessons.
- Take care with USB drives or external storage; only use devices authorised by the school.
- Log out of accounts when finished using shared or school devices.

3. Mobile Devices

- Mobile phones and personal devices must be used according to the **Mobile Phone and Electronic Devices Policy**.
- Devices should not be used to take photos, videos, or audio recordings without staff permission.
- Unauthorised or inappropriate use of personal devices may lead to them being confiscated in line with the Behaviour Policy.

4. Online Safety and Digital Citizenship

- Think before posting or sending messages; once something is online it may be permanent.
- Avoid interacting with strangers online and protect your personal information.
- Respect other people's rights, identities, and beliefs.
- Follow the school's guidance during remote lessons (Microsoft Teams/TeamViewer Meeting or other school-approved online platforms) regarding behaviour, background, and recording.
- Never create, request, send, or share sexual images or videos of yourself or others. This is unsafe and illegal, even if everyone involved has given consent.

5. Sanctions

Breaking these rules may result in:

- Temporary or permanent loss of ICT access.
- Additional disciplinary or restorative action according to the Behaviour Policy.
- In serious cases, referral to police or local authorities.

6. Related Policies

This AUP should be read alongside:

- Trust Safeguarding Policy
- Anti-Bullying Policy
- Mobile Phone and Electronic Devices Policy
- Behaviour Policy
- Data Protection Policy