



St Peter's Catholic High School & Sixth Form Centre

ICT Acceptable Use Policy - Student Version

1. Introduction and aims

This document is a simple version of the main ICT Acceptable Use Policy. If you wish to view the full AUP you can do so via the school website (www.sphs.uk.com)

ICT (computers, laptops, tablets, phones, and school software) is an important part of learning and school life. It helps with lessons, homework, and school administration.

This policy tells students how to **use school ICT safely and responsibly**.

It aims to:

- Explain rules for using school computers, devices, and networks
- Keep everyone safe online
- Help students learn to use technology responsibly
- Prevent misuse of school ICT

Breaches of this policy may result in disciplinary action according to the school's behaviour policy.

2. Definitions

- **ICT facilities:** School computers, tablets, laptops, phones, software, websites, apps, and other digital tools
- **Users:** Any student authorised to use the school ICT facilities
- **Personal use:** Using ICT for things unrelated to schoolwork
- **Authorised personnel:** Staff allowed to manage or monitor ICT systems
- **Materials:** Files, photos, videos, documents, or other data created using school ICT

3. Unacceptable use

Students must **not use school ICT** to:

- Break copyright or intellectual property laws
- Bully, harass, or discriminate against others
- Break school rules
- Access, create, or share inappropriate, offensive, or pornographic content
- Share nude or semi-nude images/videos (sexting)
- Defame or damage the reputation of the school
- Share confidential school information
- Hack, access restricted areas, or use passwords that are not yours
- Install software or apps
- Damage school devices or data
- Bypass school filters
- Promote a private business
- Use AI tools (e.g., ChatGPT) to do homework, assessments, or coursework and claim it as your own

4. Access to ICT facilities

- Computers and specialist equipment can only be used **under staff supervision**
- Sixth Form students may use the Sixth Form computers **independently for educational purposes**
- Students must follow staff instructions when using ICT

5. Searches and deletion of material

School staff may **search devices** if there are reasonable grounds to suspect:

- Risk to staff or pupils
- Evidence of an offence

This includes inappropriate images, abusive messages, or evidence of crime.

- Students may be asked to **delete material** if it could cause harm or break rules
- Devices containing **indecent images of children** must be handed to staff **without viewing or sharing**
- Staff will follow **safeguarding and legal guidance** if searching or deleting material

6. ICT use outside school

Students may face **sanctions** for using ICT irresponsibly outside school, including:

- Cyberbullying or harassment
- Sharing inappropriate content or nude images/videos
- Illegal activity or encouraging illegal activity
- Misuse of passwords or unauthorised access
- Damage to ICT systems or data
- Posting material that could harm the school's reputation

7. Monitoring

The school **monitors ICT use** to:

- Keep students safe
- Make sure ICT is used responsibly
- Investigate breaches of school rules
- Protect the school systems and data

Monitoring may include:

- Websites visited
- Emails and messages sent
- Computer activity
- Access to school ICT systems

Students should understand that **ICT use is not private** and will be checked when necessary.



8. Internet and WiFi

- School WiFi is filtered and secure
- Sixth Form students may use WiFi for schoolwork when permitted by staff
- Internet use must be **for learning purposes only**
- Students must **report any failures in filtering** to staff

9. Cyber security

Students must:

- Keep passwords secure and never share them
- Follow staff instructions on protecting school devices
- Report suspicious emails, messages, or websites

10. Behaviour online

- Be respectful and responsible online
- Don't post or share content that could harm others
- Follow the rules for using social media, messaging apps, and online platforms

11. Related policies

This policy should be read with:

- Behaviour Policy
- Safeguarding Policy
- E-Safety Policy
- Data Protection Policy
- AI (Artificial Intelligence) Policy

