

Purbrook Park School

Enjoy Enrich Excel



Acceptable Use of IT and Online Safety Policy (Pupils)

Coordinator: Director of Inclusion

Start Date: September 2025

Review Date: September 2026

Contents:

Statement of intent

1. Purpose
2. Core Principles
3. Safe and Responsible Use
4. Online Communication and Conduct
5. Images, video and audio
6. Data Protection and Privacy
7. Academic honesty and AI tools
8. Personal Devices (BYOD) if applicable
9. Monitoring and Filtering
10. Reporting Concerns
11. Sanctions for Misuse
12. Monitoring and Review

Statement of intent

Purbrook Park school believes that Information Technology (IT) plays an important part in both teaching and learning over a range of subjects, and the school accepts that school-owned devices are widely used by pupils. The school is committed to ensuring that pupils have access to the necessary facilities and support to allow them to carry out their work.

This IT Acceptable Use Agreement and Online Safety Policy outline the rules and guidelines for the use of the school's Information Technology (IT) resources by all pupils who attend the school. By using the school's IT resources, you agree to abide by the terms and conditions outlined in this document. The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Pupils are responsible users and remain safe while using the internet
- School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Pupils are protected from potential risks in their everyday use of electronic devices.

This policy should be read in conjunction with the School's Behaviour Policy.

1. Purpose

This policy explains how pupils are expected to use school IT systems and the internet safely, responsibly, and respectfully. The aim is to:

- keep pupils safe online and on school devices
- protect the school's network, data, and equipment
- promote positive digital citizenship and learning

This policy applies to all pupils using:

- school computers, laptops, tablets, and other devices
- the school network, Wi-Fi, and internet access
- school email, learning platforms, and digital services
- any personal device used on the school site or for schoolwork (where permitted)

2. Core Principles

When using IT at school, pupils must:

1. Be safe – protect themselves and others online.
2. Be respectful – treat others appropriately in digital spaces.
3. Be responsible – use systems for learning and follow instructions.
4. Be honest – act with integrity and do not attempt to deceive or bypass rules.

3. Safe and Responsible Use

Pupils must:

- Use school IT only for learning activities and school-approved purposes.
- Always follow staff instructions when using devices or the internet.
- Keep personal information private (e.g., full name, address, phone number, passwords).
- Tell a member of staff immediately if they see anything worrying, inappropriate, or unsafe online.
- Log off or lock the device when leaving it unattended.
- Treat school equipment carefully and report damage or faults promptly.
- Use respectful language and behaviour when communicating online

Pupils must not:

- Access, share, search for, or display inappropriate material, including content that is violent, sexual, hateful, extremist, or otherwise unsuitable.
- Bully, harass, threaten, mock, or embarrass anyone online or through digital tools.
- Upload, post, or forward images or videos of anyone without their permission.
- Use another person's account, login, or password.
- Attempt to bypass school security or filters, including by using VPNs, proxies, TOR, hotspots, or "portable" software.
- Download or install software/apps/games without staff permission.
- Deliberately damage, interfere with, or misuse school devices or network services.
- Use IT for gambling, illegal activity, or any activity that brings the school into disrepute.

Failure to comply with this IT Acceptable Use Agreement and Online Safety Policy may result in disciplinary action, in line with the School Behaviour Policy

4. Online Communication and Conduct

When using email, Teams/Google Classroom/learning platforms, forums, or chats:

- Communication must stay polite, relevant to learning, and appropriate.
- Pupils must not send abusive messages, spam, chain messages, or content intended to upset others.
- Pupils must not create or join groups that exclude, mock, or target others.
- Any concerns about online behaviour (including outside school) can be reported to staff and may be treated as a safeguarding issue.

5. Images, video and audio

- Pupils may only record or photograph on school devices when a member of staff has agreed and for genuine learning purposes.
- Sharing or posting recordings/images of pupils or staff without consent is not permitted.
- Any misuse of images (including humiliating, sexualised, or threatening content) will be treated as a serious breach of our IT and Behaviour Policies, and may involve safeguarding leads or external agencies.

6. Data Protection and Privacy

To protect everyone's information:

- Pupils must store work only in school-approved locations (e.g., OneDrive/Google Drive) and not on random websites or personal accounts unless directed.
- Pupils must not access staff-only areas, confidential files, or data about other pupils.
- Pupils must not copy, edit, or share school data without permission.

7. Academic honesty and AI Tools

The school encourages technology to support learning, and integrity is important.

Pupils must:

- Produce their own work unless collaboration is specifically allowed by staff.
- Reference sources when using information from the internet.
- Use AI tools (if allowed for a task) only within the boundaries given by the teacher.

Pupils must not:

- Submit AI-generated work as their own where this is not explicitly allowed.
- Use AI/chatbots to bypass learning, assessments, or restrictions.
- Upload personal or sensitive school information into public AI systems.

Teachers will clarify when AI/support tools are permitted and how they should be used.

8. Personal Devices (BYOD) if applicable

If pupils are allowed to bring personal devices:

- Personal devices must only be used with staff permission and for learning.
- Devices must connect only to the school's approved pupil Wi-Fi.
- The same rules in this policy apply to personal devices on school premises.
- Staff may require a device to be switched off or handed in if misuse occurs.

9. Monitoring and Filtering

To keep pupils safe:

- The school uses filtering and monitoring systems.
- Internet use may be supervised and logged.
- Any concerning searches, content, or messages may be flagged to staff, including Designated Safeguarding Leads.

10. Reporting Concerns

Pupils should report immediately if:

- they see upsetting or unsafe content
- someone asks them for private information
- they feel threatened or bullied online
- they think a login/password has been compromised
- they are worried about a friend's online safety

They can speak to any trusted adult, their tutor, Year Leader, or a Designated Safeguarding Lead.

11. Sanctions for Misuse

Breaches of this policy will be dealt with in line with the Behaviour Policy and may include:

- verbal warning and re-teaching of expectations
- temporary removal of IT privileges
- detentions, isolation, suspension and/or exclusion
- parental contact
- device confiscation (personal or school)
- involvement of safeguarding staff
- referral to external agencies where required (e.g., police)

Serious incidents include (but are not limited to): deliberate access to harmful content, cyberbullying, sharing indecent images, harassment, extremist material, or attempts to compromise the network.

12. Monitoring and Review

This policy will be reviewed bi-annually.

Any changes or amendments to this policy will be communicated to pupils and parents.

The scheduled review date for this policy will be September 2027.