

# IT Services Governance

## Acceptable Use Policy - Pupils



# Sheldon School

BE KIND | BE BRAVE | BE THE BEST YOU

## Working in partnership with



Leadership Responsibility: <b>Chief Operating Officer</b>	Effective Date: <b>October 2025</b>
Governors' Committee Responsible: <b>Resources</b>	Review Date: <b>October 2026</b>

## Contents

Introducing our Acceptable Use Policy for Pupils .....	3
Personal credentials.....	3
Keeping technology safe and working .....	3
Use of media .....	3
Communication.....	4
Use of internet .....	4
Artificial Intelligence (AI) tools.....	4
Acceptable Use .....	4
Not Acceptable Use .....	4
Bringing your own device to school.....	5
Monitoring .....	5

## Introducing our Acceptable Use Policy for Pupils

Our Acceptable Use Policy helps students understand how to use school technology responsibly and safely. It sets clear rules for using devices, internet access, and online tools—like not sharing personal information, avoiding inappropriate content, and respecting others online. By following this policy, students help create a positive learning environment and protect themselves and others. Everyone is expected to use technology in a way that supports learning, follows school values, and keeps our digital spaces safe and respectful.

## Personal credentials

### All pupils must:

- Only log on with the username and password you were given.
- Always log off after you have finished. If you find a computer logged in to with someone else's account credentials please log it off.
- Never let anyone else know your password. Never attempt to log on using someone else's username or send email from someone else's account.
- Must change your password regularly in line with advice from the ICT department. If you think someone else knows your password, please tell the ICT department.

## Keeping technology safe and working

### All pupils must:

- Not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Not take part in any activity that threatens the safety of the school IT systems, or activity that attacks or corrupts other systems, is forbidden.
- Inform the ICT department if they think there is a virus on the system.
- Not attempt to install or remove software on any workstation or make changes to its configuration.
- Not attempt to access data belonging to other students or staff.

## Use of media

### All Pupils must:

- Not take pictures or record film of any students or members of staff, while in school or on school trips, without the permission of those being photographed or filmed.
- Not take unauthorised photographs or video of other students or staff. Do not share such images without the express permission of all involved.
- Respect copyright materials. Do not save pictures, music or video files unless you have created them yourself. Doing so may break the author's copyright.
- Not use their phones, without explicit permission from a member of staff, is forbidden and phones should be kept turned off and in bags at all times.

## Communication

**Pupils are responsible for all emails sent from their own account and must ensure, at all times, they:**

- Do not engage in 'chat' or social networking activities over the school Internet.
- Use appropriate language.
- Do not send, or encourage others to send, abusive messages.
- Do not use language that could cause hatred against any ethnic, religious or another minority group.
- Must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Must not post anonymous messages and forwarding chain letters is forbidden: Pupils will not be allowed access to public, unregulated chat rooms.

## Use of internet

Pupils must acknowledge that all internet activity on their accounts is monitored by the school to ensure their safety.

**All Pupils must:**

- Not attempt to access inappropriate websites such those promoting violence, racist views or pornographic websites. You should inform your teacher if you are able to access such sites from within the school.
- Not use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.

## Artificial Intelligence (AI) tools

Sheldon recognises the growing role of AI in education and encourages its responsible use to support learning, creativity and digital literacy. Pupils may use AI Tools (e.g., chatbots, generative platforms, translation software) only under the following conditions:

### Acceptable Use

- To support homework, revision and research
- To enhance creativity in writing, design or coding
- As accessibility tools (e.g., speech-to-text, translation)
- When directed by a member of staff for specific tasks

### Not Acceptable Use

- To plagiarise or submit AI-generated work as their original
- To generate inappropriate, harmful, or misleading content
- To bypass learning or assessment expectations
- To share personal data with external AI Platforms

## Bringing your own device to school

If you bring your own ICT equipment to school

- It remains your responsibility. The school isn't responsible if it's not working, damaged, lost, or stolen.
- You may only use mobile devices, including wearable technology such as smart watches, when a member of staff gives you specific permission to use them in their class, and only for school purposes. Otherwise, these should remain switched off in your bag during the school day.
- If permitted, you must connect the equipment to the internet through the school's GUEST wireless network.
- You must not connect your equipment to the school's ICT equipment unless you have permission from the ICT Support team.
- You must protect your device with a passcode, password, or biometric authentication if you are using it to log in to school ICT services. Passcodes or passwords must be different to those you use anywhere else.

## Monitoring

The school reserves the right to enforce these restrictions by monitoring email and computer use. Any monitoring carried out is for the purposes of safeguarding and security. Files stored on the school's systems will be checked regularly and deleted without warning if deemed unsuitable or a risk to the security of the school's network and IT services.

You are responsible for your actions in and out of school. Therefore:

- Consequences will be given if you misuse school ICT systems, or behave inappropriately outside of school in a way that is linked to your membership of our community, e.g. cyberbullying.
- Staff may confiscate any technology, including mobile devices or USB sticks, if they believe it has been used inappropriately.
- If there are any parts of this policy that you don't understand, you should ask a member of staff for advice.