



ICT & Social Media Acceptable Use Policy 2026-2027

Document Control - Document Details	
Document Name	ICT & Social Media Acceptable Use Policy
Document Version number	2
Document Owner	Faye Hatchard
Prepared by	Faye Hatchard
Document Location	College Policies/Approved Policies 2025-2026
Date of first draft	September 2025
Date Approved	September 2026
Approved by	Governing Body
Next scheduled review date	September 2027

Version History		
Version Number	Date Approved	Change/reason for change/comments

Distribution List
Governors
Head
Leadership Team

Please refer to the separate Artificial Intelligence (AI) Policy.

Introduction

Oathall Community College recognises that access to technology provides students, staff and visitors with greater opportunities to learn, engage, communicate, and develop skills that prepare them for work, life, and citizenship. We are committed to helping all users develop responsible, safe, and ethical use of 21st-century digital tools.

To that end, Oathall provides access to a range of technologies. This Acceptable Use Policy outlines the behaviours and expectations for all users of our ICT systems, ~~AI tools~~, and social media platforms. It applies when using **school-owned devices, personally owned devices on school premises, and official college platforms or accounts.**

The college network and digital systems are intended primarily for **educational purposes**. All activity over the network **may be monitored and retained** in line with safeguarding, legal, and security requirements.

Technologies Covered

This policy covers all technology and online services provided by Oathall, including but not limited to:

- Internet and Wi-Fi access
- Desktops, laptops, tablets, and mobile devices
- Email and collaboration tools (Google Workspace including Gmail, Drive, Classroom)
- Learning platforms, online assessments, and video conferencing
- Social media and official Oathall accounts (Facebook, X/Twitter, Flickr)
- Artificial Intelligence tools and apps where approved for learning purposes

As new technologies emerge, Oathall will evaluate their use and update this policy accordingly.

Usage Policies

All technology use must reflect the following principles:

- **Be safe** – protect yourself and others online.
- **Be respectful** – online conduct should match the expectations of offline behaviour.
- **Be responsible** – treat devices, accounts, and information carefully.
- **Be ethical** – follow copyright, academic honesty, and safeguarding rules.

Misuse of school resources can result in disciplinary sanctions.

Web & Online Content

- Internet access is filtered to protect users. Attempts to bypass filters are prohibited.
- Web browsing is monitored and logs may be retained.
- Research must be conducted using reputable sources; users should be mindful of misinformation.

Email

- Every student receives a **school Gmail account** for official use.
- Email should be used **politely and professionally**, and only for educational purposes.
- Communication with staff should occur during appropriate times (not during holidays).
- Email is monitored and for safeguarding.

Learning Platforms, Collaboration & Social Media

- Oathall provides collaborative tools (Google Drive, Classroom, messaging functions). Posts, chats, and shared content may be monitored.
- Users should not share personal or identifying information online.
- Only **authorised staff accounts** may post on official Oathall social media.
- Personal social media accounts must not be used to contact or follow pupils.
- Personal social media accounts must not be used to search for and make contact with pupils, staff or any member of the Oathall community.

Mobile Devices

- School-issued devices must be treated with care; loss or damage must be reported immediately.
- Personally-owned devices, such as laptops or tablets, may only be used in school with the explicit permission of a member of staff and where their use supports learning or an identified additional need (e.g. a SEND provision or medical need).
- This permission does not apply to mobile phones, smart phones or smart watches, which are governed by the College's Mobile Phones & Devices Policy. Students must not use personal mobile phones during the school day unless an agreed exception applies.
- Users are financially responsible for negligence leading to device damage.

Security & Downloads

- Users must safeguard against malware and phishing. Suspicious messages should be reported immediately.
- Downloading executable files (.exe) or unauthorised applications is forbidden.
- Files may only be downloaded from trusted sources for educational purposes.

Netiquette & Online Behaviour

- Treat others with respect online. Cyberbullying, harassment, or discriminatory behaviour will not be tolerated.
- Be aware that once something is posted online, it can be permanent.
- You must not post or email anything which could cause distress or offence, is inaccurate or which could constitute illegal behaviour.

Plagiarism & Copyright

- Users must not copy content from the internet without giving credit.
- Copyright law applies to all online content, including images, videos, music, and text.
- AI-generated content must be used responsibly and cited appropriately.

Personal Safety

- Never share personal information online (address, phone, financial details).
- Do not arrange to meet online contacts in person without parental permission.
- Report anything unsafe or inappropriate immediately to a member of staff.

Cyberbullying & Online Harassment

Cyberbullying and online harassment in any form is strictly prohibited. In some cases, such behaviour may be considered a criminal offence. Any form of cyberbullying or harassment that takes place in school or through the use of school IT systems will result in disciplinary action.

Unacceptable behaviours include, but are not limited to:

- Harassment, intimidation, or repeated unwanted contact.
- Spreading malicious or abusive rumours and gossip.
- Sending threatening or intimidating messages via email, text, or online platforms.
- Mobbing (a group or gang targeting an individual).
- Intimidation, blackmail, or coercion.
- Stalking or continual online harassment.
- Posting embarrassing, humiliating, or explicit images or videos without consent.
- Sharing private or personal details online without consent.
- General bullying or stalking through digital means.
- Grooming (enticing or encouraging harmful, criminal, or self-destructive behaviour).
- Creating false profiles, identity fraud, or identity theft.
- Using online gaming platforms to bully, harass, or attack others.
- Theft, fraud, or deception conducted online.

All incidents will be managed in accordance with the college's Behaviour & Anti-Bullying Policy and, where appropriate, may be escalated to the police or other relevant authorities.

Limitation of Liability

While Oathall employs filtering and security systems, the college cannot guarantee their effectiveness. Oathall is not responsible for unauthorised transactions or damages resulting from misuse of technology.

Consequences of Violations

Behaviour that is unacceptable offline is equally unacceptable online. Sanctions may include:

- Loss or suspension of ICT access
- Notification to parents/carers
- Detention, exclusion, or other disciplinary measures
- Legal action where appropriate

Examples of Acceptable Use

I will:

- Use ICT for learning, research, and school-related activities.
- Communicate respectfully and courteously online.
- Protect myself and others by reporting harmful or inappropriate content.
- Treat equipment carefully and report problems promptly.
- Credit sources correctly and respect copyright.
- Use AI responsibly, with teacher approval and transparency.

Examples of Unacceptable Use

I will not:

- Use ICT to bully, harass, or harm others.
- Attempt to bypass filters or security settings.
- Plagiarise or misuse AI to cheat in assessments.
- Download unauthorised or harmful software.
- Post or share personal/identifying information online.
- Use ICT for illegal, obscene, or disruptive activities.