CARDIFF SIXTH FORM COLLEGE CAMBRIDGE

Dukes EDUCATION

IT Acceptable Use Policy

August 2026

Document Quality Control

Original

Version	Author	Date	Reviewed By	Date
Version 1	David Fear	May 2022	Gareth Collier	May 2022

Document Reviews/Updates

Document Version Editing	Reason for Review/Update	Reviewer	Date	Checked / Approved By	Date
May 2022	Annual Update	Julian Davies	July 2023	Chris Sweet	August 2023
August 2023	Annual Update	Julian Davies	August 2024	Chris Sweet	August 2024
August 2024	Annual Update	Julian Davies	September 2025	Clair Curtis-Dyke	September 2025
August 2026	Annual Update	Julian Davies	18/08/2026	Clair Curtis-Dyke	18/08/2026

Contents

1.0 Introduction

1.1 Cardiff Sixth Form College (CSFC) Cambridge prides itself on its innovative approach to the use of ICT. We are progressive in our approach and wholeheartedly encourage the sensible use of technology in all the teaching and administrative functions of the college.

1.2 This policy applies to all College ICT systems, online services, internet access, email, artificial intelligence tools, social media platforms, communication technologies, personal devices and any associated digital resources used by staff or students.

1.3 This policy relates to all staff, governors, visitors and students. It is inclusive of both fixed and mobile internet technologies provided by the college (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc). It includes technologies owned by students and staff, but brought onto college premises (such as laptops, mobile phones and other mobile devices).

1.4 This policy, supported by the college's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole college community. It is linked to the following mandatory college policies: Safeguarding and Child Protection, Anti-Bullying, Online Safety and Prevent.

2.0 Data Security

2.1 Commitment to Data Security

Cardiff Sixth Form College (CSFC) Cambridge recognises that it processes and stores personal, confidential and commercially sensitive information relating to students, parents, staff and other members of the College community. All users of College ICT systems are responsible for ensuring that information is handled securely and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and College policies.

2.2 Access to College Information

Access to College systems and information is provided solely for authorised educational and operational purposes. Users must only access information that is necessary for their role and must not attempt to access information, systems or accounts for which they have not been granted permission.

2.3 Authentication and Account Security

Users must:

- Keep passwords, passphrases, passkeys and authentication credentials confidential.

- Use strong and unique passwords for College accounts.
- Enable Multi-Factor Authentication (MFA) where provided by the College.
- Never share user accounts or allow another person to access College systems using their credentials.
- Immediately report any suspected compromise of an account or password.

2.4 Protecting College Information

Users must take reasonable steps to protect College information at all times. This includes:

- Locking devices when left unattended.
- Ensuring devices are protected with appropriate security controls.
- Storing information only within approved College systems and platforms wherever possible.
- Exercising caution when accessing College systems from personal or public devices.
- Minimising the downloading or local storage of College information.

2.5 Personal Devices and Cloud Services

The use of personal devices is governed by the College Bring Your Own Device (BYOD) Policy.

College information must not be stored on personal devices, personal cloud storage accounts or unapproved applications unless authorised by the College and protected by appropriate technical and organisational safeguards.

Users must ensure that any automated backup facilities do not result in College information being transferred to unauthorised personal cloud services.

2.6 Encryption and Data Transfer

Personal, confidential and special category personal data must be protected using appropriate security measures, including encryption, access controls and approved College systems.

Users should avoid sending personal or confidential information by email wherever a secure sharing platform is available.

2.7 Artificial Intelligence

Staff and students must not upload confidential, personal, safeguarding-related or commercially sensitive College information to publicly available or consumer artificial intelligence systems unless explicitly authorised by the College and covered by appropriate contractual and data protection safeguards.

Staff and students using artificial intelligence tools must comply with the College's Academic Integrity, Assessment and Data Protection requirements and any guidance issued by teaching staff. Users remain responsible for the accuracy, appropriateness and integrity of any work supported by artificial intelligence.

2.8 Security Incidents and Data Breaches

Any actual or suspected:

- data breach;
- loss of College information;
- loss or theft of a device containing College information;
- malware infection;
- unauthorised access attempt; or
- compromise of a College account

must be reported immediately to the Operations Manager and the GDPR Champion and no later than 24 hours after discovery.

2.9 Monitoring and Compliance

The College reserves the right to monitor the use of its ICT systems where there is a legitimate safeguarding, operational, regulatory, legal or security reason to do so and in accordance with applicable legislation.

Monitoring will be proportionate, conducted in accordance with applicable legislation and used only for legitimate College purposes.

Users should be aware that information created, stored, transmitted or received through College systems may be accessible to authorised personnel where necessary.

Failure to comply with this policy may result in disciplinary action and, where appropriate, the withdrawal of access to College ICT facilities.

3.0 Email and Electronic Communications

3.1 College email is an essential communication tool and must be used professionally, responsibly and in accordance with this policy.

3.2 The College provides email accounts for staff and students for educational and operational purposes. College email accounts must be used for all College business.

Staff must not use personal email accounts to communicate with students, parents or third parties on College matters.

3.3 Users must:

- Keep their account credentials secure and confidential.
- Use only their own College account and never access or use another person's account.
- Ensure that all communications are professional, accurate and appropriate.
- Check carefully that emails are addressed to the intended recipients before sending.
- Share personal, confidential or special category personal data only where there is a lawful basis and legitimate educational or operational need.
- Use College-approved secure file-sharing systems in preference to email attachments where available.
- Report suspicious, malicious or inappropriate emails immediately.
- Comply with all College policies when accessing email from personal devices or off-site location

3.4 Users must not:

- Forward emails or attachments unnecessarily.
- Send offensive, abusive, discriminatory or inappropriate content.
- Use College email for unauthorised commercial, political or personal promotional activities.
- Use personal email accounts for College business.

3.5 Emails and other electronic communications created, sent or received through College systems may be retained, reviewed or disclosed where required for safeguarding, legal, regulatory, operational or security purposes and in accordance with applicable legislation.

4.0 Professional Conduct Online

4.1 Staff must maintain professional boundaries and act in a manner consistent with their responsibilities as employees of the College.

4.2 Staff must not:

- Interact with current students through personal social media accounts.
- Share confidential, safeguarding-related or personal information.
- Publish content likely to bring the College into disrepute.
- Post images of students without authorisation.

4.3 Staff are expected to use privacy settings appropriately and exercise professional judgement in all online interactions.

5.0 Online Safety

5.1 The College is committed to promoting the safe, responsible and effective use of technology.

5.2 Online Safety is embedded within the curriculum, student induction programme, staff training, safeguarding arrangements and pastoral support systems.

5.3 Students are taught how to manage online risks, including cyberbullying, privacy, misinformation, harmful content, online exploitation and the responsible use of technology.

5.4 Staff are expected to:

- Model safe and responsible online behaviour.
- Reinforce Online Safety messages where appropriate.
- Maintain professional boundaries online.
- Report Online Safety concerns in accordance with safeguarding procedures.

5.5 Online bullying, harassment or intimidation, including cyberbullying, will not be tolerated and will be managed through the College safeguarding and behaviour procedures.

5.6 Further guidance is contained within the College Online Safety Policy.

6.0 Inappropriate Material

6.1 Users who accidentally access inappropriate content must report the incident immediately to a member of staff or line manager, as appropriate.

6.2 Deliberate access to illegal, harmful or inappropriate material may result in disciplinary action and, where appropriate, referral to external agencies.

7.0 Internet Use

7.1 College internet access is provided to staff and students to support education, learning, research and operational activities.

7.2 Users must:

- Use internet services responsibly and lawfully.
- Comply with safeguarding, data protection and academic integrity requirements.

- Follow staff instructions regarding appropriate use.
- Protect login credentials and personal information.
- Report inappropriate content, security concerns or suspected misuse.

7.3 Users must not:

- Access illegal or inappropriate content.
- Attempt to bypass filtering, monitoring or security controls.
- Download unauthorised software.
- Use College systems to bully, harass or discriminate against others.
- Use College systems for unauthorised commercial, political or gambling activities.

7.4 The College reserves the right to restrict access where misuse is identified.

8.0 Devices and Digital Content

8.1 Users must use College and personal devices responsibly and in accordance with safeguarding and data protection requirements:

- Personal devices should only be used for College purposes where authorised.
- Staff should use College communication systems whenever possible.
- Images of students may only be taken in accordance with College procedures.
- Images stored on personal devices must be transferred to authorised College storage and deleted, including from cloud backups, within 72 hours.
- Mobile phones and cameras must never be used in changing areas.
- College equipment is provided for educational and operational purposes and must not be used for unauthorised personal activities.
- College data stored on portable devices must be appropriately protected.

9.0 ICT Code of Conduct

By using College ICT systems, I agree to:

- Use technology responsibly and respectfully.
- Protect my account credentials.
- Protect personal and confidential information.
- Follow safeguarding, data protection and academic integrity requirements.
- Report concerns or misuse promptly.
- Respect copyright and intellectual property.

- Avoid attempting to bypass security controls.
- Use College systems only for authorised purposes.

I understand that misuse may result in restrictions, disciplinary action or referral to external authorities where appropriate.