



# Digital Communications and Social Media Policy

## 1. Purpose

The College recognises the benefits and opportunities new technologies offer for teaching, learning, and assessment. This policy details the approach the College takes to identify and manage risks, safeguard staff and students, and promote the safe use of technology. It ensures all digital activity reflects College values, complies with legal requirements, and protects the privacy of our community.

## 2. Scope

This policy applies to all students, staff, partners, sub-contractors, and members of the Board of Governors. It covers all use of the internet and electronic communication tools, including but not limited to:

- Email, mobile phones, tablets, and games consoles.
- Social networking sites (e.g., TikTok, Instagram, YouTube).
- Collaboration tools, personal publishing, and AI systems.

---

## 3. Key Principles

### 3.1 Respect and Professionalism

- All content shared must be respectful, accurate, and appropriate.
- Content must never put any student or staff member at risk physically, emotionally, or reputationally.
- Users must not post anything that could damage the reputation of the College, its staff, or students.
- Any content associating a user with the College, such as wearing a uniform, displaying a lanyard, or having identifiable signage in the background, must reflect College values and maintain professionalism.

### 3.2 Acceptable Use and ICT Security

- All users must adhere to the standards of behaviour set out in the ICT Acceptable Use Policy.

- Digital communications, including email and internet postings over the College network, are monitored.
- Security measures, including firewalls, anti-virus software, and encryption, are maintained to protect users and the institution.

### **3.3 AI Usage Guidelines**

- AI tools may only be used in compliance with the ICT Acceptable Use Policy.
  - Personal data or sensitive College information must not be entered into AI tools unless explicitly authorised.
  - The generation or sharing of misleading, offensive, or fraudulent content via AI is strictly prohibited.
  - Users are encouraged to critically evaluate and verify AI-generated content for accuracy and appropriateness.
- 

## **4. Social Media and Content Creation**

### **4.1 Filming and Photography on Campus**

- Filming or photographing on College grounds, in classrooms, or during College-organised trips/work placements is prohibited without prior permission from a tutor or line manager.
- Interviewing or filming other students or staff for personal platforms (e.g., TikTok, Instagram, YouTube) requires prior permission from the individuals involved and the College.
- Before posting permitted content, users must review it for safeguarding risks, such as visible ID cards, registers, sensitive documents, or background conversations revealing personal info.
- Avoid humour or language that could be misinterpreted or cause harm.
- Do not tag students or staff in posts unless they have agreed.
- Avoid posting content that could indicate a student's location at a specific time or reveal vulnerable circumstances (e.g., health issues).

### **4.2 Professional Boundaries**

- Staff using social networking to communicate with students must do so only on a professional basis using College-managed or approved sites.
  - Groups set up under the College name must use a College email account and follow the staff Code of Conduct.
  - Staff must not "friend" students within personal social networking environments or share personal information with them.
  - Communications must maintain professional boundaries to ensure the staff member's professional position is not compromised.
-

## 5. Data Protection and Safeguarding

### 5.1 Personal Data

- The College collects and stores personal data in line with UK-GDPR legislation.
- Users must not share personal information about themselves or others without explicit and official College written consent.
- Never share student records, contact details, or confidential information regarding College operations and assessments.

### 5.2 Image and Video Consent

- The consent of individuals pictured in College activities is sought prior to publication.
  - If consent is granted, individuals must understand how the content will be used and retain the right to withdraw it at any time.
  - Special care must be taken regarding images of minors (students under 18) or vulnerable individuals.
- 

## 6. Incident Management and Consequences

### 6.1 Reporting Concerns

- **Students:** Report incidents to a Personal Tutor, Programme Management, or Head of School.
- **Staff:** Report incidents through a line manager.
- **Immediate Action:** If a safeguarding risk is spotted in existing content, report it immediately to the Designated Safeguarding Lead (DSL)
- **Remediation:** Remove or edit content promptly if a risk is identified.

### 6.2 Consequences of Misuse

- Unacceptable conduct or failure to comply with this policy will be treated seriously and may lead to disciplinary action under College Codes of Conduct.
  - Actions may include removal of content, suspension, or referral to external authorities (such as the police) if laws are breached.
- 

## 7. Responsibilities

- **Head of IT / Systems Development:** Responsible for managing ICT infrastructure and data security.
- **Deputy Principal / Head of Student Services:** Responsible for managing Safeguarding arrangements.
- **All Staff and Students:** Responsible for ensuring their practice and use of College systems is compliant with this policy