Oakswood College

Empowering Through Education

# Social Media and IT Acceptable Use

*Policy*

PROMOTING EXCELLENCE • ENSURING COMPLIANCE
SUPPORTING OUR COMMUNITY

GOVERNANCE | QUALITY | COMPLIANCE | EXCELLENCE

www.oakswoodcollege.co.uk

Oakswood College
Empowering Through Education


*(Trading name of Oakswood Group Ltd)*

# Social Media & IT Acceptable Use Policy

**Document Control & Version History**

| Field | Details |
|---|---|
| Document Title | Social Media & IT Acceptable Use Policy |
| Document Type | Governance Policy |
| Policy Owner | Head of Governance, Quality, Compliance & Information Systems |
| Accountable Officer | Chief Executive Officer |
| Approved By | Board of Governors |
| Approval Date | 25 September 2025 |
| Effective From | 25 September 2025 |
| Review Cycle | Annual |
| Next Review Date | 25 September 2026 |
| Version Number | 1.0 |
| Supersedes | New Policy |
| Applies To | All staff, students, governors, contractors, and third-party users of Oakswood CollegeIT systems |
| Regulatory Reference | Data Protection Act 2018; UK GDPR; Computer Misuse Act 1990; OfS Conditions of Registration (E2 – Management & Governance); Prevent Duty (Counter-Terrorism and Security Act 2015) |
| Location | Staff Intranet / Website / Governance & Policy Repository |
| Related Documents | IT & Digital Systems Policy; Data Protection Policy; Business Continuity Policy; Freedom of Speech Policy; Staff Code of Conduct; Student Code of Conduct; Disciplinary Policy |

Oakswood College
Empowering Through Education

## Contents


1. Purpose ..... 4

a) Ensure Responsible and Safe Use ..... 4

b) Safeguard Students, Staff, and the Oakswood College Community ..... 4

c) Protect Oakswood College Data, Systems, and Reputation ..... 4

d) Support Regulatory and Legal Compliance ..... 4

e) Facilitate Efficient IT Resource Management ..... 4

f) Provide a Framework for Enforcement and Assurance ..... 5

Cross-References: ..... 5

2. Scope & Applicability ..... 5

2.1 Who This Policy Applies To ..... 5

2.2 Systems and Resources Covered ..... 5

2.3 Applicability ..... 5

3. Acceptance of Policy ..... 6

3.1 Requirement to Comply ..... 6

3.2 Confirmation of Acceptance ..... 6

3.3 Specific User Groups ..... 6

3.4 Ongoing Responsibility ..... 6

3.5 Withdrawal of Access ..... 7

4. Principles of Acceptable Use ..... 7

4.1 Core Principles ..... 7

4.2 Expected User Behaviour ..... 7

4.3 Prohibited Use ..... 7

4.4 Personal Use ..... 7
4.5 Governance & Accountability ..... 7
5. Acceptable Use of IT Resources ..... 8
5.1 Primary Purpose ..... 8
5.2 Access & Credential Security ..... 8
5.3 Device & Network Security ..... 8
5.4 Reporting & Incident Management ..... 8
5.5 Responsible Digital Conduct ..... 8
5.6 Governance & Accountability ..... 8
6. Security-Sensitive Materials & Prevent Duty Compliance ..... 8
7. Social Media Use ..... 9
7.1 Official Oakswood College Accounts ..... 9
7.2 Personal Accounts ..... 9
7.3 Security & Governance of Official Accounts ..... 9
8. Monitoring & Privacy ..... 10
9. Safeguarding & Data Protection ..... 10
10. Reporting Misuse ..... 10
10.1 What Must Be Reported ..... 10
10.2 How to Report ..... 10
10.3 Responsibilities ..... 11
11. Consequences of Violation ..... 11
12. Review & Updates ..... 12
13. Process Flowchart ..... 12

## 1. Purpose

This policy establishes standards and expectations for the acceptable use of Oakswood Oakswood College IT/ERP systems, networks, devices, digital services, and online platforms (collectively referred to as "IT Resources"). It provides a governance framework to protect users, the College, and its community.

This policy is in place to:

**a) Ensure Responsible and Safe Use**

- Promote responsible, ethical, and lawful use of IT resources by all users.
- Protect the College, staff, students, and third-party partners from misuse, cyber threats, and unsafe digital practices.

**b) Safeguard Students, Staff, and the Oakswood College Community**

- Support compliance with safeguarding obligations and the Prevent Duty.
- Establish clear guidelines for identifying, handling, and reporting security-sensitive materials.
- Reduce risks of online harassment, exposure to inappropriate content, and misuse of sensitive information.

**c) Protect Oakswood College Data, Systems, and Reputation**

- Ensure integrity, confidentiality, and availability of Oakswood College data and IT systems.
- Prevent unauthorised access, disclosure, or loss of sensitive information, including personal, academic, and administrative data.
- Maintain the College's reputation through guidance on professional digital communication and social media use.

**d) Support Regulatory and Legal Compliance**

- Align with relevant legislation: UK GDPR, Data Protection Act 2018, copyright and intellectual property laws, anti-discrimination laws, and Prevent Duty obligations.
- Meet Office for Students (OfS) expectations regarding digital systems, governance, and data management.

**e) Facilitate Efficient IT Resource Management**

- Ensure IT resources are used primarily for legitimate Oakswood College purposes.
- Promote awareness of responsibilities, including password security, incident reporting, and acceptable online conduct.

**f) Provide a Framework for Enforcement and Assurance**

- Establish foundations for monitoring, auditing, and enforcing IT compliance.
- Support disciplinary, contractual, and regulatory responses where misuse occurs.

**Cross-References:**

- Data Protection Policy and Procedure
- Date Privacy Notice
- Prevent & Safeguarding Policy
- Staff and Student Codes of Conduct
- Cyber Security & Business Continuity Policy

## 2. Scope & Applicability

This policy applies to **all users of Oakswood Oakswood College IT resources**, including systems, networks, devices, software, data, and online platforms, **regardless of location or device**.

### 2.1 Who This Policy Applies To

- Applicants to any programme of study.
- Enrolled students.
- Staff (permanent, temporary, fixed-term, agency, contractors, consultants).
- Applicants to Oakswood College staff positions during recruitment, onboarding, and induction.
- Governors, trustees, volunteers, and visitors granted authorised IT access.
- Third-party partners, contractors, and service providers with authorised access under contractual agreements.

### 2.2 Systems and Resources Covered

- Oakswood College desktop/laptop computers, mobile devices, and servers
- Email, messaging, and collaboration systems
- Virtual Learning Environment (VLE), student portals, and online platforms
- Data storage, databases, and cloud services
- Network infrastructure, Wi-Fi, and remote access tools
- Any other authorised Oakswood College IT, digital, or online service

### 2.3 Applicability

- Policy applies **on and off Oakswood College premises**, including remote work or personal device use.
- Users are responsible for compliance whenever accessing Oakswood College IT resources.
- Non-compliance may result in disciplinary action, access withdrawal, or referral to authorities.

## 3. Acceptance of Policy

Compliance with this policy is **mandatory** for staff and students of Oakswood Oakswood College to gain and maintain access to Oakswood College IT systems.

### 3.1 Requirement to Comply

Before access is granted, users must:

- Receive this policy and be informed of mandatory compliance
- Acknowledge potential consequences of non-compliance

Compliance obligations:

- **Staff:** Part of contractual and professional obligations
- **Students:** Part of Student Code of Conduct and enrolment conditions
- **Contractors/Third Parties:** Part of contractual/service agreement

### 3.2 Confirmation of Acceptance

- Electronically: via login, onboarding portal, or learning platform declaration
- In writing: during enrolment, induction, or contract documentation
- Continued use constitutes **deemed acceptance** if formal confirmation is not obtained.

### 3.3 Specific User Groups

- **Staff:** Acknowledge during induction; access may be withheld until acknowledgement; breaches handled via Staff Disciplinary Procedure.
- **Students:** Acknowledge during enrolment or IT account activation; breaches addressed under Student Conduct & Discipline Procedure.
- **Third Parties:** Must acknowledge compliance prior to authorised system access.

### 3.4 Ongoing Responsibility

- Users must remain familiar with the current policy and comply with updates.

- The Oakswood College may amend the policy to reflect legal, regulatory, operational, or security changes.

### 3.5 Withdrawal of Access

- IT access may be suspended or withdrawn for misuse, security risk, or policy breaches.
- Re-acknowledgement may be required after significant updates.

## 4. Principles of Acceptable Use

All users must use IT resources **responsibly, ethically, and safely**.

### 4.1 Core Principles

- **Protect Individuals & the College:** Prevent harm, avoid unauthorised disclosure, safeguard operations and reputation.
- **Comply with Legal Obligations:** Adhere to GDPR, safeguarding, Prevent, equality, copyright, and licensing rules.
- **Reflect Oakswood College Values:** Support integrity, accountability, respect, and professional conduct.

### 4.2 Expected User Behaviour

- Align IT usage with professional and academic responsibilities
- Avoid illegal, offensive, discriminatory, or inappropriate material
- Respect privacy and dignity of others
- Promptly report suspected misuse, breaches, or safeguarding concerns

### 4.3 Prohibited Use

- Personal financial gain or commercial use
- Extremist, pornographic, or offensive material
- Sharing login credentials
- Bypassing security controls
- Cyberbullying or harassment
- Installing unlicensed software

### 4.4 Personal Use

- Permitted only if lawful, reasonable, and non-disruptive
- Subject to monitoring and Oakswood College security obligations

### 4.5 Governance & Accountability

- Users are accountable for actions and may face disciplinary action
- Oakswood College may monitor and restrict access to protect users, systems, and compliance

## 5. Acceptable Use of IT Resources

### 5.1 Primary Purpose

- Academic, teaching, research, administrative, and operational activities
- Limited personal use permitted under 4.4

### 5.2 Access & Credential Security

- Secure login credentials, strong passwords, multi-factor authentication, lock unattended devices, avoid unsecured storage

### 5.3 Device & Network Security

- Use only authorised College-managed devices
- Follow security updates, licensing, and software requirements
- Report lost or compromised devices immediately

### 5.4 Reporting & Incident Management

- Report phishing, unauthorised access, data disclosure, malware
- Timely reporting prevents escalation and supports compliance

### 5.5 Responsible Digital Conduct

- Avoid illegal or inappropriate material
- Respect intellectual property
- Maintain professional communication
- Protect privacy and dignity of others

### 5.6 Governance & Accountability

- Breaches may result in withdrawal of access, disciplinary action, or legal notification
- Users are accountable for all actions using Oakswood College IT credentials

## 6. Security-Sensitive Materials & Prevent Duty Compliance

- Materials that impact safeguarding, student welfare, or national security (e.g., extremist content) must be **handled only as authorised**

- Refer to Prevent & Safeguarding Policy for identifying, reporting, and managing materials
- **Report concerns immediately** to the Prevent SPOC, Designated Safeguarding Lead or IT Services

**Examples:**

Extremist propaganda, safeguarding records, restricted research, sensitive student/staff data

**Governance:**

Breaches may result in disciplinary action, access withdrawal, or law enforcement notification

**Cross-References:**

Prevent & Safeguarding Policy, Data Protection Policy, Staff/Student Codes of Conduct

## 7. Social Media Use

### 7.1 Official Oakswood College Accounts

- Only authorised staff may manage accounts
- Content must align with Oakswood College mission, values, communications strategy, and comply with all policies
- Posts should avoid controversy unless approved; copyright-compliant; timely responses; strong password + MFA

### 7.2 Personal Accounts

- Freedom of expression is upheld but must not breach law, contracts, or Oakswood College policies
- Staff and students must not:
    - present personal views as Oakswood College views;
    - disclose confidential info, or
    - engage in harassment
- Users may be perceived as representing the Oakswood College when using Oakswood College branding or identifying as staff/student

### 7.3 Security & Governance of Official Accounts

- Account creation approved by Head of Governance, Quality, Compliance & Information Systems or senior manager

- Designated Account Owner responsible for oversight
- Central register maintained; personal emails not permitted
- MFA and strong passwords required
- Access logging, annual review, prompt revocation for role changes or suspected compromise
- Content backup where feasible

## 8. Monitoring & Privacy

- Lawful, fair, transparent monitoring of college-owned devices, networks, email, VLEs, cloud services, and official social media accounts
- Monitoring applies onsite and remotely, including limited personal use
- Purpose: network security, safeguarding, misconduct investigation, compliance, performance
- Methods: automated network analysis, email filtering, logs, social media review, account/device investigation
- Evidence may be used in disciplinary or safeguarding investigations
- Monitoring will **not suppress lawful academic debate or whistleblowing**

## 9. Safeguarding & Data Protection

- Compliance with UK GDPR, Data Protection Act 2018, and Oakswood College Data Protection Policy
- Users must process personal data lawfully, limit access, keep data accurate, report breaches immediately
- Safeguarding responsibilities: protect students, staff, vulnerable individuals, report concerns promptly to DSL or Prevent SPOC
- Prevent Duty: report extremist material or radicalisation concerns immediately
- Online conduct is an extension of in-person conduct; breaches may result in disciplinary action

## 10. Reporting Misuse

### 10.1 What Must Be Reported

- Security incidents: phishing, malware, unauthorised access
- Policy breaches: IT misuse, social media, systems
- Content concerns: offensive, discriminatory, extremist
- Safeguarding, Prevent, or security-sensitive issues

### 10.2 How to Report

Staff and students can report any concerns, incidents or allegations via one of the following routes:

- IT Services (technical/security)
- Prevent SPOC (radicalisation/extremist concerns)
- DSL (safeguarding/welfare)

Anonymous reports are allowed, but reporting parties are encouraged to identify themselves to facilitate full and proper investigations

Reporting parties are asked to provide the following information as far as they are able when making a report:

- dates
- times
- systems
- accounts
- content
- evidence

**10.3 Responsibilities**

- Users must cooperate fully with investigations
- Staff with managerial or IT responsibilities must escalate and record incidents
- Confidential handling per UK GDPR, safeguarding, and Prevent obligations

## 11. Consequences of Violation

| Breach Type | Potential Consequences | Responsible Authority |
|---|---|---|
| Minor/Accidental | Additional training, guidance, monitoring | Line Manager / IT Services |
| Serious/Intentional | IT access withdrawal, disciplinary action (Non-Academic Misconduct Policy for students; Staff Disciplinary Policy for staff) | DSL / IT Services / Senior Management |
| Legal/Regulatory Breach | Referral to police or legal action | CEO / Board |

- All users must report security incidents, policy violations, or IT/social media misuse (please see Section 10 of this Policy)

## 12. Review & Updates

- Annual review or earlier if required due to:
  - Legislation, regulatory, or guidance changes
  - Technology or cybersecurity developments
  - Best practice updates or audit findings
- Board of Governors approves substantive amendments; CEO may approve minor/technical updates with reporting to Board
- Updates recorded in Version History, communicated to stakeholders, and published in the official policy repository

## 13. Process Flowchart

1. **User Identifies Issue** – Any student, staff, contractor, or third-party noticing a breach, misuse, offensive content, or IT problem.
2. **IT / System Misuse** – Includes hacking, phishing, malware, password sharing, unauthorised software, or general IT policy violation.
3. **Safeguarding / Prevent Issue** – Includes welfare concerns, radicalisation, extremist content, harassment, or safety-related material.
4. **Responsible Roles:**
   - **IT Services:** Investigation, technical mitigation, access control
   - **DSL (Designated Safeguarding Lead):** Safeguarding and welfare
   - **Prevent SPOC:** Radicalisation and extremist content concerns
   - **CEO / Board:** High-risk, serious incidents escalation
5. **Outcome / Consequence Paths:**
   - **Minor / Accidental:** Guidance, training, monitoring
   - **Serious / Intentional:** Disciplinary action, withdrawal of IT access, legal escalation
   - **Extreme / High-Risk:** Referral to law enforcement or regulatory bodies