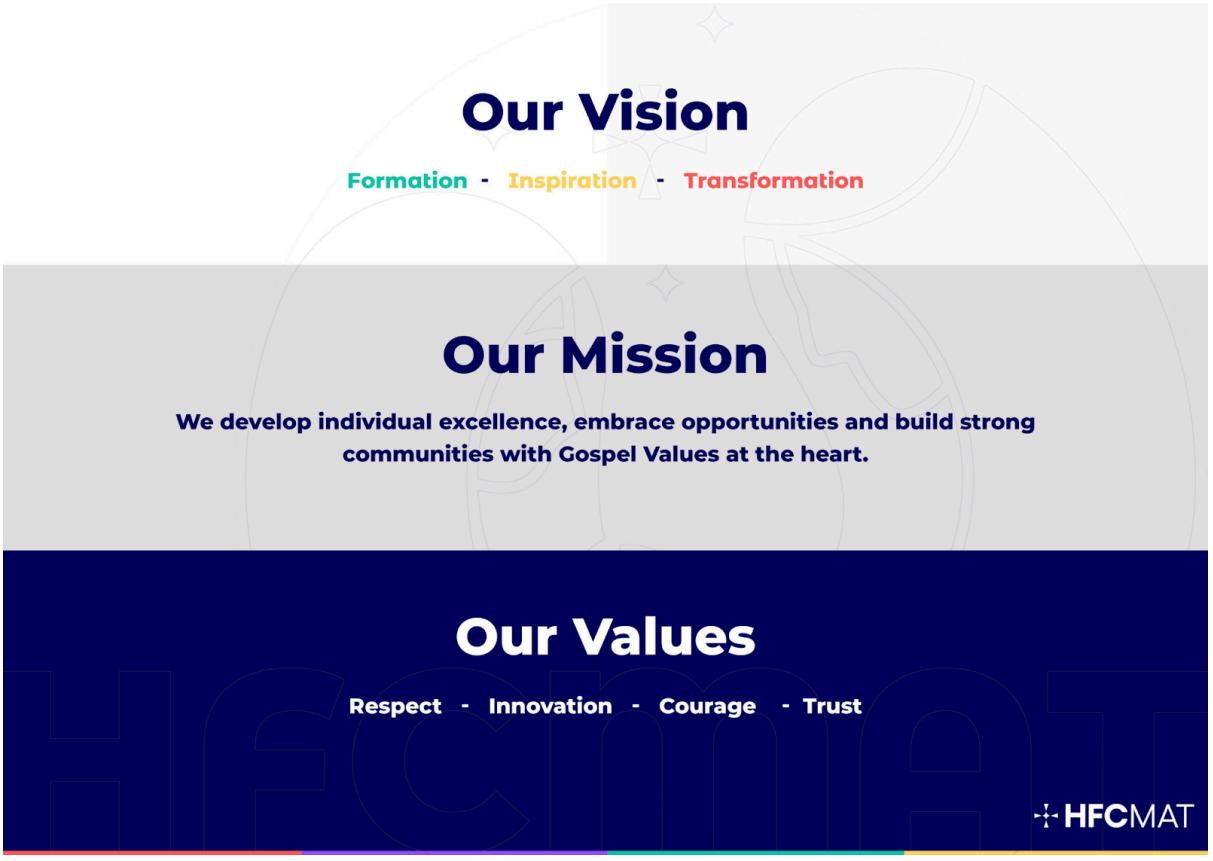
Acceptable Use of IT and Electronic Communications Policy



Document Management

Policy name:	HFCMAT Acceptable Use of IT and Electronic Communications Policy		
Approved by:	Audit, Risk & Resources Committee	**when:**	Spring 2026
Review by:	Operations Manager	**when:**	Spring 2028
File location:			
Version control:	New policy from Hi Impact, Spring 26		

Acceptable Use of IT & Electronic Communications Policy

1. Introduction and Aims

Information Technology (IT) and electronic communications are integral to the efficient and safe operation of the Trust. Our systems support teaching and learning, safeguarding, pastoral support, administration, and communication across all Trust schools.

However, the use of IT and communications systems carries inherent risks relating to data protection, online safety, safeguarding, and reputational risk. This combined policy establishes the standards expected of all users and ensures compliant and responsible use of Trust systems.

This policy aims to:

- Provide clear rules and expectations for the acceptable use of all Trust IT systems and electronic communications.
- Ensure compliance with data protection, online safety, safeguarding and cyber security requirements.
- Protect the Trust, our schools, staff, pupils and stakeholders from misuse or unlawful activity.
- Prevent disruption, data breaches, reputational damage or operational interruption.
- Ensure that pupils are taught to use technology safely, respectfully and responsibly.
- Establish a consistent Trust-wide approach for monitoring, sanctions and oversight.

This policy applies to all users of Trust IT systems, including staff, governors, volunteers, contractors, visitors, parents and pupils.

Breaches of this policy may lead to disciplinary, behavioural, contractual or safeguarding action as appropriate.

2. Relevant Legislation and Guidance

This policy reflects and complies with:

- Data Protection Act 2018
- UK GDPR
- Computer Misuse Act 1990
- Human Rights Act 1998
- Telecommunications (Lawful Business Practice) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education
- DfE Searching, Screening and Confiscation Guidance

This policy should be read alongside the Trust's:

- Data Protection Policy
- Child Protection & Safeguarding Policy
- Online Safety & Mobile Phone Policy
- Behaviour Policy
- Disciplinary and Capability Procedure
- Staff Code of Conduct

3. Definitions

IT Facilities
All systems, hardware, software, cloud services, data storage, networks, Wi-Fi, telephony, email, communication platforms, devices and future technologies provided by the Trust.

Users
Anyone authorised to access Trust IT facilities (staff, governors, volunteers, contractors, visitors, parents, and pupils).

Electronic Communications
Email, messaging services, telephony, video conferencing, cloud-based collaboration, online platforms and digital communications related to Trust business.

Personal Use
Any use not directly related to Trust employment or school purpose.

Authorised Personnel
Staff designated to administer, monitor or manage IT systems (e.g., IT support, Trust/School leadership).

4. Unacceptable Use

The following behaviour is prohibited. Breaches may lead to disciplinary or behavioural sanctions:

4.1 Prohibited Activities

Users must not:

- Breach copyright or intellectual property rights.
- Bully, harass, discriminate or intimidate others.
- Access, create, store, or share pornographic, extremist, offensive or inappropriate material.
- Conduct illegal activity or advocate illegal actions.
- Share confidential or personal information without authorisation.
- Access or attempt to access restricted areas, systems, files or passwords.
- Introduce malware, attempt to bypass security, or interfere with system functioning.
- Install, connect or use unauthorised software, web services or devices.
- Defame or bring the Trust or its schools into disrepute.
- Use offensive, aggressive or inappropriate language.
- Promote a private business unless authorised.

- Use personal email or personal devices to store or transmit Trust data (unless explicitly authorised).
- Bypass or attempt to bypass Trust web filtering or security.

4.2 Electronic Communications Requirements

Users must:

- Use Trust email accounts for all work-related communication.
- Ensure communication is professional, accurate and appropriate.
- Encrypt attachments containing sensitive or personal information.
- Not use personal accounts to communicate with parents or pupils.
- Not share personal phone numbers with parents or pupils unless written approval is given.
- Report misdirected emails or potential data breaches immediately.
- Understand that emails may be subject to disclosure (FOI, SAR, legal proceedings).

5. Sanctions

Breaches of this policy may result in:

- Restricted or withdrawn access to IT systems
- Behaviour sanctions for pupils
- Disciplinary action for staff
- Referral to LADO or safeguarding authorities where appropriate
- Reporting to police where criminal activity is suspected

Repeated or serious breaches may result in formal disciplinary proceedings in line with Trust procedures.

6. Staff Use (Including Governors, Volunteers and Contractors)

6.1 Access and Accounts

- All staff receive user accounts, logins and access rights appropriate to their role.
- Staff must keep passwords secure and must not share login credentials.

6.2 Email, Telephony and Communications

- Trust email must be used for all work-related business.
- Personal devices may only be used with explicit written approval and must meet encryption and security standards.
- Personal email addresses must not be used for Trust business.
- Staff must not store personal data on local drives or unencrypted devices.
- Phone calls with parents must be made using school-provided equipment unless authorised.

6.3 Personal Use

Permitted only when:

- It does not occur during contact time
- No pupils are present
- It does not interfere with work or network performance
- It does not fall under unacceptable use
- No personal files (e.g. photos/music) are stored on Trust systems

6.4 Remote Access

- Staff must abide by all parts of this policy when accessing systems remotely.
- Devices must be locked and protected from unauthorised access.

7. Pupils

7.1 Access

Pupil access to IT resources is determined by each school.

7.2 Searching & Deletion

Schools may search devices and delete stored data where legally permitted and appropriate (Education Act 2011).

7.3 Misuse Outside School

Schools may sanction pupils for off-site misuse of IT or social media if it impacts the school, pupils, staff or the Trust.

8. Parents

8.1 Access

Parents do not have access to IT systems unless explicitly authorised in an official capacity.

8.2 Online Conduct

Parents must:

- Communicate respectfully with staff online
- Use appropriate channels (not pupil accounts)
- Follow school rules on social media engagement

9. Data Security

9.1 Passwords

- Must be strong and updated every 12-18 months.
- Must not be shared.

9.2 Software & Virus Protection

- Users must not disable firewalls or antivirus systems.
- Devices update automatically and users must allow these updates.

9.3 Encryption

- USB sticks must not be used.
- Trust data must be stored only on Google Workspace or other approved systems.

9.4 Access Control

Users must:

- Only access information they are authorised to access
- Lock screens when not in use
- Log out fully at end of day

10. Internet Access and Filtering

The Trust provides filtered, safeguarded internet access.
Staff must not share Wi-Fi passwords with unauthorised users.

- Guest or parent access requires headteacher approval.
- Inappropriate websites must be reported immediately.

11. Monitoring

The Trust reserves the right to monitor:

- Internet use
- Emails
- Telephony
- System access logs
- User activity

Monitoring is for:

- Compliance
- Safeguarding
- Preventing crime
- Operational security
- Legal obligations (FOI, SAR, investigations)

12. Review

This policy will be reviewed every two years, or earlier if legislation changes.