All Saints
Catholic Academy Trust

Acceptable Use

Policy Author:	C Reffold
Policy Lead (if applicable):	Director of Governance & Compliance
Responsible Committee:	Audit and Risk
Date of Policy:	October 2025
Date approved:	December 2025
Review Cycle:	Annual
Date for Review:	October 2026
Location of policy:	Compliance
Intended Circulation:	All Staff
Version	1.0

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to define clear standards for the responsible, secure, and lawful use of the All Saints Catholic Academy Trust's (ASCAT) information systems, networks, and digital resources.

This policy ensures compliance with the **Cyber Security Policy**, **Online Safety Policy**, and **Data Protection Policy**, and supports the Trust's mission to provide a safe, ethical, and digitally secure learning and working environment.

2. Scope

This policy applies to:

- All ASCAT staff, governors, trustees, contractors, volunteers, and temporary workers;
- All pupils using Trust systems or devices;
- Any third parties or service providers with access to Trust networks or data.

It covers all use of Trust-provided equipment, personal devices connected to Trust systems, cloud services, and any data created, accessed, or transmitted through Trust platforms.

3. Policy Aims

The aims of this policy are to:

- Protect the confidentiality, integrity, and availability of Trust information and systems;
- Ensure all users understand their responsibilities;
- Promote safe, respectful, and ethical use of digital technology;
- Safeguard pupils and staff from cyber and online risks;
- Maintain compliance with legal and regulatory requirements.

4. Legal and Policy Framework

This policy operates within the framework of:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Computer Misuse Act 1990**
- **Safeguarding and Prevent legislation**
- **Education Act 2011**
- **ASCAT Cyber Security Policy**
- **ASCAT Online Safety Policy**
- **ASCAT Data Protection Policy**

5. Roles and Responsibilities

5.1 Trust Board and Senior Leadership

- Approve and oversee implementation of this policy.
- Ensure adequate resources for cyber security and data protection.

- Monitor compliance and respond to breaches.

5.2 Data Protection Officer (DPO)

- Provide advice on data protection and information governance.
- Oversee compliance with data protection legislation.
- Support the handling of data breaches and subject access requests.

5.3 IT Services

- Manage system access, technical security, and monitoring.
- Maintain the security of networks, servers, and endpoint devices.
- Support users in reporting and resolving cyber incidents.

5.4 Staff, Governors, and Volunteers

- Use Trust IT systems responsibly and lawfully.
- Follow the principles in this and related policies.
- Report any concerns, breaches, or cyber incidents immediately.

5.5 Pupils

- Use technology safely, respectfully, and only for learning.
- Follow the Pupil Acceptable Use Agreement.
- Report anything that makes them feel unsafe or uncomfortable online.

6. Acceptable and Unacceptable Use

6.1 Acceptable Use

Users must:

- Access Trust systems only for approved educational or business purposes.
- Use their own login credentials and keep them secure.
- Protect all Trust data in accordance with the Data Protection Policy.
- Communicate professionally in all Trust-related digital correspondence.
- Follow staff or teacher instructions regarding online activity.

6.2 Unacceptable Use

Users must not:

- Share passwords or access credentials.
- Access, modify, or share data without authorisation.
- Install unauthorised software or use unapproved cloud storage.
- Visit or share inappropriate, offensive, or illegal content.
- Use Trust systems for personal gain, political lobbying, or commercial purposes.

- Engage in online bullying, harassment, or discrimination.
- Attempt to disable or bypass security controls, filtering, or monitoring systems.

7. Use of Trust Devices

- Trust-issued devices remain Trust property at all times.
- Only authorised software and configurations may be used.
- Users must not alter or attempt to repair Trust devices.
- Devices must be protected with passwords and encryption.
- Devices must be returned when employment or enrolment ends.

8. Personal and Bring Your Own Devices (BYOD)

- Personal devices may only access Trust data if authorised by the IT Team and secured appropriately.
- Pupils may use personal devices only when permitted and under supervision.
- Personal devices used for Trust purposes must:
    - Have up-to-date security software;
    - Use strong passwords;
    - Never store or process personal data unless explicitly approved.

9. Remote Working

When working remotely, staff must:

- Use only Trust-managed systems (e.g., Microsoft 365).
- Store data on secure cloud drives, not local storage.
- Keep devices in secure physical locations.
- Dispose of printed information securely.

10. Data Protection and Privacy

All users must comply with the **ASCAT Data Protection Policy**:

- Only collect and use personal data necessary for their role.
- Share information securely and lawfully.
- Report any suspected data breach immediately to the DPO.
- Keep confidential data secure and avoid unauthorised disclosure.
- Never upload or enter personal or sensitive data into AI tools unless explicitly authorised following a **Data Protection Impact Assessment (DPIA)**.

11. Online Safety and Digital Behaviour

Aligned with the **ASCAT Online Safety Policy**, all users must:

- Communicate respectfully and responsibly online.

- Protect themselves and others from harmful content or behaviour.
- Report online safety concerns (e.g., cyberbullying, grooming, or harassment).
- Avoid publishing Trust-related images or information on personal social media without consent.
- Seek parental permission (for pupils) before using online services requiring consent.

12. Monitoring and Filtering

- ASCAT monitors the use of IT systems to ensure compliance, protect users, and prevent misuse.
- Internet filtering systems block access to inappropriate or harmful content.
- Monitoring is conducted lawfully, proportionately, and in accordance with the Data Protection Act 2018.

13. Cyber Security

All users must support the Trust's cyber resilience by:

- Completing mandatory cyber security training annually.
- Being alert to phishing, social engineering, and fraudulent communications.
- Avoiding public or unsecured Wi-Fi networks with Trust devices.
- Promptly reporting suspected security incidents to the IT Team.

14. Reporting and Incident Management

If a user suspects a cyber, data, or safeguarding incident, they must:

1. **Stop using the affected system** immediately.
2. **Report** it to the IT Team, Headteacher, and DPO without delay.
3. **Follow instructions** provided by the Trust's Cyber Response and Recovery Plan.

Incidents may include:

- Phishing attempts;
- Data loss or unauthorised disclosure;
- Device theft or compromise;
- Malware or ransomware infection.

15. Training and Awareness

- All staff and governors must complete annual cyber and data protection training.
- Pupils will receive digital literacy and online safety education appropriate to their age.
- Periodic exercises (e.g., phishing simulations) will test awareness.

16. Breach of Policy

Non-compliance with this policy may result in:

- Withdrawal of system access;
- Disciplinary action under the relevant Staff or Behaviour Policy;
- Legal action or referral to external authorities in serious cases.

17. Monitoring, Review, and Approval

This policy will be reviewed annually by the **Director of Governance & Compliance**, **Data Protection Officer**, and **IT Services**, and approved by the **Audit & Risk Committee**.

Monitoring will ensure:

- Ongoing compliance with legislation;
- Regular updates to reflect evolving cyber and data risks;
- Consistency with Trust safeguarding and data protection procedures.

18. Linked Policies and Documents

- **ASCAT Cyber Security Policy**
- **ASCAT Online Safety Policy**
- **ASCAT Data Protection Policy**
- **Behaviour Policy (Schools)**
- **Safeguarding and Child Protection Policy**
- **Disciplinary Policy**
- **Records Management and Retention Schedule**
- **The Safe Use of AI**