All Saints
Catholic Academy Trust

Acceptable Use Agreement – Staff & Governors

1. Purpose

This Acceptable Use Agreement outlines the responsibilities of staff, governors, and other authorised users in ensuring the secure, ethical, and lawful use of the Trust's IT systems, networks, and data.

It supports compliance with the **ASCAT Cyber Security Policy**, **Data Protection Policy**, and **Online Safety Policy**.

2. Scope

This agreement applies to:

- All employees, governors, volunteers, contractors, and temporary workers using Trust systems.
- Any device that connects to the Trust's network, including Trust-provided equipment and authorised personal devices.

3. Professional Conduct and Compliance

All users must:

- Use IT systems **for legitimate Trust purposes only**.
- **Comply with UK GDPR, the Data Protection Act 2018, and the Computer Misuse Act 1990**.
- **Protect the confidentiality, integrity, and availability** of Trust data.
- Adhere to all relevant Trust policies, including the **Cyber Security Policy** and **Online Safety Policy.**

4. Security and Access Control

You must:

- Keep passwords secure and never share them.
- Use **strong passwords** and enable **Multi-Factor Authentication (MFA)** where available.
- Lock or log out of devices when unattended.
- Report lost or stolen devices immediately to the **IT Team**, **Headteacher**, and **Data Protection Officer (DPO)**.
- Only use authorised Trust accounts for work — not personal email or storage platforms.
- Never install unauthorised software, apps, or browser extensions on Trust devices.

- Not attempt to bypass or disable Trust security controls or filtering systems.

5. Use of Devices

- Trust-provided devices are for professional use only.
- Devices must remain managed and configured by the Trust's IT Team.
- Do not connect devices to public Wi-Fi networks such as cafés or hotels.
- Devices must not be taken outside the UK without written approval from the **Approvers** (CEO, CFO, or Headteacher).
- Personal use of Trust systems should be minimal and must not breach Trust policy or compromise security.

6. Bring Your Own Device (BYOD) and Remote Work

- Only Trust-managed devices may access Trust data or email systems.
- Personal devices must not store, process, or transmit Trust data unless specifically authorised and configured securely.
- Staff should not use third party platforms to transfer documents or information.
- When working from home:
    - Keep devices in a secure location;
    - Ensure family members or others do not use Trust devices;
    - Avoid printing personal data unless necessary and dispose of it securely.

7. Data Protection

All users must:

- Handle all information in line with **data protection principles**.
- Only access, share, or store data that is relevant to their role.
- Use encrypted storage and secure cloud platforms approved by the Trust (e.g., Microsoft 365).
- Report any suspected or actual **data breach** immediately to the **DPO**.
- Not forward Trust data to personal accounts or third-party platforms.

8. Communication and Online Conduct

Users must:

- Communicate professionally and respectfully in all Trust communications.
- Avoid sending messages or posting content that could harm the Trust's reputation.
- Follow the **Online Safety** and **Social Media Policies**.
- Ensure all communications about pupils or staff are confidential and appropriate.

9. Monitoring and Privacy

The Trust reserves the right to:

- Monitor and log system activity to maintain network integrity and compliance.
- Access information stored on Trust systems when required for safeguarding, legal, or operational reasons.

All monitoring will be lawful and proportionate in line with the Data Protection Act 2018.

10. Cyber Awareness and Training

- Staff and governors must complete mandatory cyber and data protection training at induction and at least annually.
- Periodic phishing and awareness exercises will be conducted to ensure preparedness.
- Everyone must familiarise themselves with the **Cyber Response and Recovery Plan**.

11. Reporting Incidents

If you suspect a cyber-security incident, phishing attempt, or unauthorised access:

- **Immediately report it** to the IT Team, Headteacher, and DPO.
- Do not attempt to investigate or resolve the issue yourself.
- Follow incident procedures set out in the Cyber Security Policy.

12. Breach of Agreement

Failure to comply with this agreement may result in:

- Withdrawal of access to IT systems;
- Disciplinary action under the **Disciplinary Policy**;
- Notification to relevant authorities where a breach of law has occurred.

13. Declaration

I confirm that I have read, understood, and agree to comply with the All Saints Catholic Academy Trust Acceptable Use Agreement.
I understand that failure to do so may lead to disciplinary or legal action.

Name Role Signature Date