Our Lady and All Saints Catholic Multi Academy Company

Staff Acceptable Use Policy (AUP)

Ratified by:	Board of Directors
Date ratified:	29.04. 2026
Name of originator/author:	Ben Clayton – January 2026
Issue Date:	04.05.2026
Review date:	March 2028

OLAAS MAC — Staff Acceptable Use Policy (AUP)

(To be read alongside the OLAAS Data Protection Policy, Information Security Policy, Online Safety Policy, Staff Code of Conduct, AI Policy and Staff Mobile Phone Policy)

1. Introduction

This Acceptable Use Policy sets out how all staff must use Trust digital systems, devices, accounts and data. It exists to safeguard pupils, protect staff, maintain secure operations across all OLAAS schools, and ensure compliance with UK GDPR, the Data (Use and Access) Act 2025, Keeping Children Safe in Education (2025), and DfE Digital & Technology Standards.

This policy applies to all staff, governors, volunteers, contractors and visitors using Trust systems.

Use of personal devices is subject to strict conditions (see Section 6.2).

Compliance with this policy is a contractual requirement. Failure to follow it may result in disciplinary action under the Staff Code of Conduct, up to and including dismissal.

2. Purpose

The purpose of this policy is to ensure:

- Safe, lawful and responsible use of Trust digital systems
- Protection of pupils and staff
- Consistent standards across all OLAAS schools
- Controlled and proportionate monitoring
- Clear expectations for communication, device use, AI use and remote access
- Alignment with Trust safeguarding, data protection and cyber-security requirements

3. Scope

This policy covers all Trust-managed:

- Devices (PCs, laptops, Chromebooks, tablets)
- Platforms (Google Workspace, Microsoft 365, MIS, safeguarding systems)
- Networks (wired, Wi-Fi, VPN/RDS)
- Accounts and credentials
- Data created, stored or processed on Trust systems

Staff use of personal devices is strictly limited to the conditions set out in this policy.

4. Legal & Regulatory Framework

This policy ensures compliance with:

- Keeping Children Safe in Education (2025)
- UK GDPR & Data Protection Act 2018
- Data (Use and Access) Act 2025
- DfE Digital & Technology Standards
- DfE Filtering & Monitoring Standards
- Prevent Duty
- Computer Misuse Act 1990
- Online Safety Act 2023

5. Core Staff Expectations

Staff must:

- Use Trust systems responsibly and professionally
- Protect logins, MFA codes and account credentials
- Report safeguarding, online-safety or data security concerns immediately
- Use only authorised platforms and systems
- Keep all pupil and staff information confidential
- Comply with local safeguarding procedures
- Follow cyber-security controls (passwords, MFA, updates, encryption)

Staff must not:

- Store Trust data on personal devices or personal cloud services
- Use personal email, messaging or social media for school business
- Attempt to bypass filtering, monitoring or security controls
- Access, share, store or create illegal, harmful, extremist or inappropriate content
- Access any system or data without a legitimate professional reason
- Share passwords or leave devices unlocked

Public social media content may be considered in conduct investigations where relevant to professional behaviour, safeguarding or trust and confidence.

Accessing any system or record without legitimate professional reason constitutes a data breach and may amount to gross misconduct.

6. Use of Devices

6.1 Trust-Managed Devices

Staff must:

- Use Trust devices primarily for work-related activity
- Keep devices secure on and off site
- Follow all encryption, MFA and security requirements
- Use only approved software
- Report lost, stolen or compromised devices immediately

Trust devices must not contain content that is illegal, harmful or inappropriate.

6.2 Personal Devices (BYOD)

Personal devices may only be used to access Trust email via:

- Gmail app (Google schools)
- Outlook app (Microsoft schools)

Personal devices must:

- Use a secure passcode or biometric lock
- Support remote wipe
- Have MFA enabled

Personal devices must never:

- Store, download, screenshot or forward Trust data
- Access MIS, safeguarding, SEN, HR or behaviour systems
- Be used for parent or pupil communication
- Store pupil photographs or files
- Access internal systems beyond approved email apps

Personal devices present increased safeguarding and data protection risks and are therefore subject to strict limits.

7. Personal Use of Trust Devices

Option A – Zero Personal Use (Strict Controls)

Trust devices, systems and networks must be used exclusively for work-related activity. Personal use is prohibited at all times, including during break periods or outside working hours.

Prohibited personal use includes (but is not limited to):

- Personal internet browsing
- Online shopping
- Banking and financial transactions
- Personal email or messaging
- Social media access or posting
- Streaming or entertainment sites
- Downloading or storing personal files

Any personal use of Trust systems may result in management action or disciplinary proceedings.

Option B – Limited Personal Use (Strictly Controlled)

Limited personal browsing is permitted during official break periods only, provided that:

- It is lawful and appropriate
- It does not involve social media posting or messaging
- It does not involve online shopping or financial transactions
- It does not involve streaming or high-bandwidth content
- It does not involve downloading or storing personal files
- It does not interfere with duties or system security

At all other times, Trust devices must be used only for work-related purposes.

Breaches may result in disciplinary action.

8. Communication Standards

8.1 Approved Communication

- Trust email
- MIS communication tools
- Managed Gmail/Outlook apps

8.2 Prohibited Communication

Staff must not:

- Use WhatsApp, SMS, Messenger, Instagram or personal email for school communication
- Contact pupils via personal accounts or devices
- Use AI-generated messages for parents or pupils

9. Safeguarding, Filtering & Monitoring

All digital activity may be logged to support safeguarding, cyber security, compliance and system integrity.

Monitoring is:

- Proportionate
- Limited to Trust systems
- Not used for routine performance surveillance
- Required under DfE Filtering & Monitoring Standards

Attempting to bypass filtering or monitoring is a disciplinary offence.

Immediate reporting of safeguarding concerns is mandatory.

10. Remote Access & Off-Site Working

Remote access is permitted only via Trust-approved methods, including VPN and RDS.

Only Trust-managed devices may be used for remote working.

Confidential information must not be viewed in public spaces.

Files must not be exported or saved to personal devices.

Personal VPNs, TeamViewer, AnyDesk, Chrome Remote Desktop and similar tools are prohibited.

The Trust does not require staff to work from home using personal equipment.

11. School Trip Communication Protocol

Staff may only use:

- School-issued trip phones
- Trust email via managed apps
- MIS-supported communication tools

Staff must not use:

- Personal phone numbers
- WhatsApp, SMS or social media messaging
- Personal email accounts

No screenshots, photos or storage of pupil information may take place on personal devices.

12. AI Use

Staff may use approved AI tools for planning, workload reduction and internal drafts.

Staff must not:

- Enter personal or sensitive data into AI tools
- Use unapproved AI systems
- Use AI for safeguarding records, SEND documentation, NEAs or assessments
- Use AI to generate communication to parents

All AI use must comply with the Trust AI Policy.

13. Data Protection & Security

Staff must:

- Store all data in Trust-approved locations
- Follow retention and deletion rules
- Report suspected breaches immediately
- Keep passwords unique and secured
- Never export or download Trust data to personal systems

Critical systems must be backed up at least daily.

At least one documented backup restore test must take place annually.

Accessing any system or record without legitimate reason constitutes a data breach and may amount to gross misconduct.

14. Breaches of This Policy

Breaches may result in:

- Removal of IT access
- Mandatory retraining
- Disciplinary action (up to dismissal)
- Safeguarding procedures where applicable

Any breach of core requirements may constitute misconduct or gross misconduct depending on severity.

15. Staff Declaration

"I confirm that I have read, understood and agree to comply with the OLAAS MAC Staff Acceptable Use Policy. I understand that failure to follow this policy may result in disciplinary action and/or safeguarding procedures."

Signature: _____
Name: _____
Role: _____
Date: _____

16. Cyber Security Governance & Assurance

The Trust Board retains strategic responsibility for digital safeguarding, filtering and monitoring standards across OLAAS MAC.

The Trust will:

- Conduct an annual cyber risk assessment
- Review cyber risks following significant incidents
- Maintain and test an incident response plan at least annually
- Ensure compliance with DfE Digital & Technology Standards
- Maintain appropriate firewall, endpoint protection and multi-factor authentication controls
- Maintain secure offsite or cloud-based backups
- Ensure appropriate supply chain cyber security assurance
- Appoint a senior digital lead responsible for cyber oversight

The Trust will not engage in ransomware payments.

Local governing bodies must ensure implementation of this policy within their school and escalate material cyber risks to the Trust.