Ormiston Academies Trust

Flegg High Ormiston Academy

Technology Acceptable Use Policy (TAUP) for Staff and Stakeholders

Policy version control

Policy type	Statutory
Author In consultation with	Richard Canning, Director of ICT National Director of Performance and Data, National Director of Infrastructure and Sustainability, National Director of Primary and Safeguarding, National Director of AP and Special Academies, Education Directors, Head of Safeguarding, Safeguarding Operations Manager, Data Protection and Complaints Manager, senior central IT team staff.
Approved by	National Leadership Group, July 2026
Release date	July 2026
Review	July 2027
Description of changes	▪ See Change Log table

Change Log

Reference	Change description
1.6.7	Clarified definition of 'Appropriate Person' as Principal, Director of ICT or NLG member
1.6.14	Added explicit definition of 'Stakeholders' (separate from staff)
2.6	Clarified removable storage media is discouraged and only permitted where protected by OAT IT
2.9	Added requirement for written approval via IT helpdesk before connecting personal devices on-site
3.2	Confirmed Microsoft Teams as the Trust's sole authorised platform for internal messaging
3.4 & 3.5	Updated WhatsApp guidance to define clear use and conditions are for specific, proportionate, operational need and must include an email follow up of message detail to provide audit trail.
3.6	Clarified the acceptable use of third-party platforms when joining external organisations
4.2 & 4.3	Replaced references to 'consent' with 'permission' when sharing personal data
6.2	Added guidance on out-of-hours emailing and use of delayed delivery
6.4	Changed guidance to minimisation, from anonymisation
7.1	Prohibited use of personal laptops and tablets on Trust premises
7.9	Added explicit provision for use of OAT devices for external statutory duties (e.g. Ofsted)
8 (all)	Updated BYOD section to clearly distinguish app-level controls from device access and monitoring
9 (all)	Refined social media and online professionalism expectations, including self-declaration
10.4	Expanded remote working guidance related to public places and privacy screens
12.1	Clarified breach and incident reporting routes for staff
12.5 & 13	Updated wording to clarify breaches will be assessed for disciplinary procedures.

Contents

1. Introduction and definitions

1.1. Please read the policy carefully. It contains legal obligations under the Data Protection Act and the Computer Misuse Act.

1.2. This policy is designed to outline the responsibilities of OAT staff and stakeholders when using technology (either personal devices or OAT devices), both on and off OAT premises. A separate acceptable use agreement is provided for pupils.

1.3. This policy will be reviewed every twelve months.

1.4. All staff must sign the declaration in this agreement annually to use the OAT IT Service. In the event of an update, staff will NOT be expected to sign the revised agreement but will be given a copy to review, with one calendar months' notice of the enforcement date.

1.5. Any reference to:

1.5.1. "OAT" refers to Ormiston Academies Trust, its head office, and its academies.

1.5.2. "Academy Data" or "Data" relates to data that is owned by OAT and for which OAT is the data controller.

1.5.3. "OAT Device" refers to any device owned by OAT head office or its academies.

1.5.4. "Personal Device" refers to any device that is not owned by OAT head office or its academies.

1.5.5. "Application" and "System" may refer to individual or multiple software programs, whether partly or wholly loaded onto a device, or devices, or accessed online.

1.5.6. "Authorised" or "Authorisation" refers to express permission from an "Appropriate Person".

1.5.7. "Appropriate Person" refers to the academy principal, Director of ICT, or member of NLG.

1.5.8. "Staff" refers to any person who is part of the academy or head office workforce, undertaking work for the academy where email accounts and / or access to systems are provided for them to carry out their role. This includes, but is not limited to, full and part-time staff, volunteers and apprentices.

1.5.9. "OAT IT Service" or the "IT Service", refers to all academy and head office IT staff, employed or contracted, as well as all IT processes, infrastructure, software, and hardware employed, commissioned, in use, planned and/or under consideration for implementation at OAT.

1.5.10. "IT Team" refers to the staff employed to provide technical and operational support and management of the OAT IT Service, whether in academies or head office.

1.5.11. "Remote working" means working at home, and anywhere other than an OAT academy or head office sites.

1.5.12. "Children" refers to anyone under the age of 18, and anyone over the age of 18 who is attending an OAT academy as a student.

1.5.13. "OAT DPO", "DPO", or "Data Protection Officer" refers to the trust Data Protection Officer.

1.5.14. "Stakeholders" refers to non-staff adults or organisations who, through their role or engagement with the Trust, are authorised to access or interact with Trust technology, systems, or data, and are therefore subject to this policy.

1.6. OAT retains the sole right of possession of any OAT device and may transfer the device to another user if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

2. Day to day use of technology at work

2.1. You must avoid facilitating or causing harm or distress to others when using technology.

2.2. You must not do anything to threaten the continuity, availability, safety or security of the IT Service, or its data, and will pay particular attention to the safe use of technology during remote working.

2.3. You must use technology in accordance with the relevant OAT policies and guidance, in particular the current data protection and safeguarding policies, and staff code of conduct.

2.4. You are accountable for the data and inputs you give to AI systems, as well as for using and sharing outputs in accordance with this and other OAT policies. Consult the guidance on use of AI published on OATnet.

2.5. You are responsible for protecting the provided technology and must prevent damage or tampering with equipment on OAT premises.

2.6. You must not use personal accounts, email or file storage for your work (e.g. a **personal** OneDrive, Dropbox, or Google Drive). You are instead required to use your work account, and the applications provided by OAT, when using technology. The use of removable storage is discouraged and is only permitted where compliant with sections 4 and 7 of this policy.

2.7. You must not share passwords with staff, children, or third parties, unless explicit permission has been given from the IT Team.

2.8. You must only use authorised hardware, software, and technology services in your work.

2.9. You must notify the IT Team and obtain written permission via a logged helpdesk ticket before connecting any personal devices, physically or wirelessly, within OAT premises (see section on Use of Personal Devices).

2.10. You must adhere to the law, in particular the Computer Misuse Act 1990, K GDPR and the Data Protection Act 2018.

2.11. You must not use OAT accounts or devices for conducting non-OAT business.

2.12. Always lock your device screen when stepping away, even briefly (e.g., to make a drink).

3. Authorised applications

3.1. Microsoft 365 is the official platform for secure daily productivity, communication, and file storage. Academy Google accounts and apps may be used until the switch to Microsoft 365 is finalised.

3.2. Microsoft Teams is the authorised service for all work-related messaging, collaboration, and hosted events.

3.3. Social media platforms like Facebook and Twitter must share OAT and academy news with parents, carers, and the community through one-way communication, only.

3.4. WhatsApp is a private messaging service that is not managed by OAT. It must not be used as the default or routine platform for OAT business. Microsoft Outlook e-mail and Teams remain the authorised services for work-related messaging and collaboration.

3.5. The Trust recognises that WhatsApp, or other non-authorised communication systems, may on occasion be used where there is a clear and specific operational need — for example, providing updates during a school trip or communicating urgent information about a school issue. Any such use must be followed up promptly with formal communication through an approved and auditable channel.

Where WhatsApp is used, staff must also comply with all the following requirements:

3.5.1. You use WhatsApp only when there is a clear work-related need and no more appropriate authorised OAT channel is suitable.

3.5.2. You do not share personal, confidential, or safeguarding information about children, staff, parents, carers, or other individuals in WhatsApp messages.

3.5.3. You do not use WhatsApp to make formal decisions, give formal instructions, record safeguarding matters, share files, or conduct activity that should be recorded in an authorised OAT system.

3.5.4. You ensure the content and tone of your messages complies with the Staff Code of Conduct and reflects the professional standards expected of your role.

3.5.5. You use the minimum information necessary and move any ongoing discussion, action, decision, or record into an authorised OAT system as soon as practical.

3.5.6. The device on which you send and receive messages is compliant with the relevant provisions of this policy, including Section 8 for BYOD security requirements.

3.5.7. You ensure that the latest software version and updates are installed on your device and that WhatsApp is protected with appropriate security settings, including two-step verification where available.

3.5.8. When asked by an Appropriate Person, you provide relevant messages in the format requested. Use is at the user's risk; support will not be provided by IT Teams.

3.6. You must use authorised applications if hosting or initiating communication and information for external professional groups and third parties.

3.7. Using other communication and file sharing applications is permitted when joining external platforms (e.g., Zoom, Facetime, Webex, iCloud, Dropbox). Staff do not need to pre-register their use, but must:

3.7.1. adhere as closely as possible to the same acceptable use conditions covering WhatsApp.

3.7.2. limit information and file-sharing to only what is necessary for the purpose of the activity.

3.8. Other named applications are also authorised and provided by OAT for specific purposes, such as HR, catering, curriculum delivery, and data management systems (e.g. Arbor, EveryHR, Parentpay, CPOMS).

4. Sharing and working with files and data

4.1. You must follow the requirements of the Data Protection and Freedom of Information policy when storing, sharing, and working with data (e.g. using files, emails, chat messages).

4.2. Do not share personal or confidential information unless you have explicit permission from the academy principal or a senior manager at head office.

4.3. Do not access, delete, modify, or share others' information without their permission or written approval from the principal or OAT Data Protection Officer (DPO).

4.4. Do not access explicit or inappropriate content on OAT's internet or devices unless it is required for your job and you have notified another staff member first.

4.5. You must delete any chain letters, spam and other emails from unknown sources without opening them, unless otherwise agreed with the IT Team.

4.6. OAT internet is for work only. Personal browsing is allowed during breaks if it does not violate this or other OAT policies.

4.7. No software should be installed by you onto OAT devices or into OAT systems, unless agreed by the IT Team.

4.8. You must not remove or disable any OAT hardware, software, or systems without the express permission of the IT Team.

4.9. USB devices and other removable media must not be used to store or transfer data, unless they have been encrypted **by the IT Team** and have passcode protection enabled.

4.10. You must delete all emails, files, and other data in line with the data retention policy, or when it is no longer required, or as part of an exit strategy.

4.11. You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables, or attempt to disrupt or circumvent IT security measures.

5. Support and monitoring

5.1. OAT regularly monitors device, application, and internet use for security and compliance.

5.2. All faults, incidents, and requests for assistance with technology must be directed to the IT Services helpdesk ticketing system.

5.3. If asked to provide equipment for inspection or repair, you should comply as soon as possible, providing all necessary peripheral items (e.g. charging cable, case)

6. Email, messaging and encryption

6.1. You are responsible for the appropriate use of email and other electronic messaging.

6.2. Your work email or messaging account must only be used for OAT business, with consideration of the impact upon the recipient's workload and wellbeing, including deciding to use delayed delivery when messaging out of normal working hours.

6.3. Email should be used for all formal communication, while other authorised messaging, such as MS Teams chat, can be used for less formal communication.

6.4. Please note that email is **not** a confidential means of communication. You should take care to avoid including personal information. If unavoidable, the information should be minimised (e.g. using initials, rather than a full name).

6.5. Keep your emails and messages brief, and avoid sharing previous threads with personal or confidential details.

6.6. Personal data must be protected when sent by email or other unsecure methods (like file attachments). Security measures depend on the type of data. This may include:

6.6.1. providing the document as a SharePoint or OneDrive link for named recipients, specifying the level of access (e.g. read only, edit).

6.6.2. protect the document with a password and send the password using a different communication method, such as a text message. Do not send the password in a separate email, as this is insecure.

6.6.3. use the encryption options within the software (e.g. MS Outlook), if the message is considered sensitive.

7. Use of OAT and academy devices

7.1. Only Trust-owned computers and devices are allowed for work on academy and OAT premises. Personal laptops or tablets are **not permitted on-site**. Personal mobile phones may only be used as outlined in Section 8.

7.2. Prior approval must be sought from the IT Team for the removal and remote use of OAT-owned devices in other locations. For remote roles, this would be agreed when a device is provided.

7.3. You must only use OAT-owned mobile phone handsets and numbers as your **main** work mobile phone, unless use of a Personal Device is approved by the IT Team **and** by an Appropriate Person. Approved use must follow this policy.

7.4. You must never use mobile devices to take images or videos of children, staff or parents unless **each** of the following is satisfied:

7.4.1. up to date consent for the specific purpose has been confirmed as received by the principal, in writing,

7.4.2. the device is an OAT-owned and/or managed device.

7.4.3. images or videos are immediately removed to authorised storage and deleted from the device.

7.4.4. images or videos are only processed for the activities for which consent has been received.

7.5. OAT-owned devices must not be used to send inappropriate messages, images or recordings.

7.6. You must ensure that OAT-owned devices do not contain any inappropriate or illegal content.

7.7. Removable USB drives and other storage media are not permitted, unless encrypted by IT and protected with a passcode.

7.8. You are expected to treat all OAT devices with care, by actively avoiding hazards and considering the risk of damage or failure of the device.

7.9. When undertaking statutory or professional duties for bodies outside the Trust (e.g. Ofsted, DfE), you may use an OAT-owned device only where:

7.9.1. No data owned by external parties is stored or synced to OAT systems (email, OneDrive, Teams, SharePoint), beyond what is strictly temporary for the purpose of completing the work.

7.9.2. If essential for the work, records containing data relating to the external parties are stored in a secure location for the duration of the work, accessible only by those involved in the work AND with a need to review.

7.9.3. Browser-only access to all systems is used, and all files are deleted immediately after use.

7.9.4. All externally-owned information is handled in line with the external organisation's instructions.

7.9.5. Any regular handling of external third-party data may require additional safeguards as directed by the Trust.

8. Use of personal devices (BYOD)

8.1. You are not permitted to use a personal computer, laptop or tablet, as your **main** device for work.

8.2. You may use your personal mobile on academy and OAT premises **only** if the conditions in 8.3 are met.

8.3. If an academy or OAT device isn't available for remote work, you may use your own device if the need is urgent and until one is provided, as long as:

8.3.1. use is confirmed in advance with IT staff

8.3.2. you have confirmed with IT staff that the appropriate device and app-level security controls are in place. For clarity, these controls:

- protect and contain Trust data within the relevant Microsoft 365 application (for example Teams, Outlook, or OneDrive)
- do not provide the Trust with access to any personal applications, messages, photographs, or browsing activity
- do not allow monitoring of personal device use

8.3.3. you only use authorised, web-based applications for your work (e.g. online versions of OneDrive, MS Office, Teams).

8.3.4. you seek approval from the IT Team before the device is connected to any network(s) inside the academy, or at other OAT premises.

8.3.5. a password is required to access the device, and the device is kept locked when not in use.

8.3.6. you have antivirus and antimalware protection running on the device at all times.

8.3.7. you avoid sharing the device. If unavoidable, you share only with a limited number of people in the home, using a separate account and login for each person.

8.3.8. you avoid downloading work-related files and attachments to your personal device.

8.3.9. If downloaded, work-related files, messages and attachments should be deleted immediately after use.

8.3.10. data stored on the device is encrypted.

8.3.11. you ensure the device is continually updated with all patches and updates, in accordance with guidance given by the manufacturer, the device operating system, and any installed applications.

8.4. If one or more of the conditions in section 8.3 is not met at any time, the device and/or use of the OAT applications and data will be blocked.

8.5. You must **never** store personal information relating to children or staff on a Personal Device. Accidental download or storage should be deleted immediately.

8.6. Do not use personal devices to contact academy children. Use OAT-owned mobile devices for trips or visits. Even with approved work use of your personal phone, do not give your number to students or parents. Always use official channels or block caller ID when contacting students or families.

8.7. You must ensure that no unauthorised persons, such as family members or friends, have access to any OAT data stored or accessed on any Personal Devices.

8.8. Inform the IT Team right away if your personal device is involved in a data breach, security incident, or shows signs of unauthorised tampering.

8.9. The IT Team only supports Personal Devices as stated above. Make sure you have a warranty or support agreement for any technical issues.

9. Social media and online professionalism

9.1. Please also see the Staff Code of Conduct, Child Protection and Safeguarding, Allegations of Abuse Against Staff, and Low Level Concerns policies.

9.2. When representing OAT or the academy online, share neutral opinions and avoid revealing confidential information or making comments that could harm its reputation.

9.3. OAT devices must not be used to access personal social networking sites, or communicate with children or parents through those sites, unless permission is granted by an Appropriate Person.

9.4. You must not accept requests from children or parents on personal social media unless you know them outside of work; if so, you must inform your principal (self - declaration) about any relationships with academy children or parents outside work.

9.5. You must ensure that the necessary privacy settings are applied to all your social networking accounts to avoid unauthorised access and keep your personal identity and information safe (e.g. Facebook, Twitter).

9.6. Never post or upload images or videos of children, staff, or parents, unless it is carried out in compliance with OAT Data Protection and Photography policies.

9.6.1. Do not share your home address, personal phone numbers, social media details, or personal email with children or parents. Use only authorised academy or OAT channels for all communication.

10. Remote working

10.1. The connection to the IT Service from home (e.g. remote access) and storage of OAT data must be encrypted. If uncertain, staff should seek advice from their IT team.

10.2. Keep all OAT hardware and software secure, store devices safely, and always activate password and privacy settings.

10.3. You must ensure your home or public wireless connection is secure and private, by following the instructions available on the device and given by your internet service provider.

10.4. Ensure data, information, and video calls are not seen or heard by unauthorised persons, whether in public places (e.g. cafes, trains) or at home with friends and family. Position your screen out of view from other people, use a video background, and wear a headset during online calls, being careful always to avoid mentioning personal data of staff and students where you might be overheard. The use of privacy screens is encouraged if working regularly in a public place.

11. Training

11.1. You must ensure that you participate in any digital safeguarding or online data protection training offered and remain up to date with current developments in social media and the internet.

11.2. You must complete the OAT GDPR and Cyber Security training before accessing personal data belonging to staff, children or other third parties.

11.3. You must allow an Appropriate Person to undertake audits to identify any areas of need in relation to your training.

12. Concerns, breaches, and misuse

12.1. You must immediately inform a member of the IT Team if you believe this policy has been breached, either by you, or another person. This can be done either through the IT helpdesk, by contacting the IT lead for your academy, or by contacting any member of the central office IT team.

12.2. Please give complete details of any suspected breach. Refer to the OAT Whistleblowing and Allegations Against Staff policies if needed.

12.3. Report any unsolicited or suspicious emails to the IT Team. If OAT data may be compromised, notify the DPL or DPO for investigation. If unsure, report to both IT and data protection staff.

12.4. You must inform the IT Team of any issues with devices, such as errors and alerts that may affect the security or function of the device, including on authorised Personal Devices.

12.5. Misuse of the IT Service will be investigated as a potential disciplinary issue, and action taken in accordance with the OAT Staff Disciplinary policy where appropriate.

12.6. Should you have any concerns about the equipment or processes within the IT Service, please raise them with a senior member of the IT Team.

13. Declaration

I confirm that I have read and understood the Technology Acceptable Use Policy (TAUP) – Staff and Stakeholders.

I understand that not following this policy is a potential breach of the Staff Code of Conduct and other OAT policies and may result in disciplinary action as appropriate, up to and including dismissal.

Signed: Date:

Print name: