Ormiston Academies Trust

Thomas Wolsey Ormiston Academy

Technology Acceptable Use Policy (TAUP) for Staff and Stakeholders

Policy version control

Policy type	Statutory, OAT template mandatory
Author	Richard Canning, Director of ICT
Approved by	OAT National Leadership Group, April 2025
Release date	April 2025
Review	April 2026
Description of changes	▪ Updated to include Appendix 1 for guidance on email use ▪ Reference to Appendix 1 inserted at 6.1 ▪ Inserted direction at 2.4 regarding the responsibility borne by staff when using artificial intelligence (AI) tools and systems

Contents

1. Introduction and definitions

1.1. Please read the policy carefully. As well as trying to avoid the very real security and safeguarding harm that our children and adults might suffer, this policy contains certain legal obligations under the Data Protection Act and the Computer Misuse Act.

1.2. Whilst OAT promotes the use of technology and understands the positive effects it can have on enhancing children's learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will be taken seriously and must be reported to the IT Team / principal / OAT Director of ICT, so that any necessary further action can be taken.

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

1.4. This policy will be updated as necessary to reflect best practice, or any amendments made to data protection legislation, and shall be reviewed every twelve months by OAT.

1.5. Each staff member must sign this agreement to continue using 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. This is to allow time for individuals to express any concerns or to formally recall their agreement. Clarifications, concerns, or recalls MUST be expressed in writing (e-mail is preferred) to the Appropriate Person within an academy or OAT head office.

1.6. Any reference to:

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

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

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

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

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

1.6.6. "Appropriate Person" refers to a staff member who has authority to grant permission for the area concerned. This is usually the academy principal, Regional ICT Manager, or Director of ICT.

1.6.7. "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.

1.6.8. “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.

1.6.9. “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.

1.6.10. “Remote working” means working at home, and anywhere other than an OAT academy or head office sites.

1.6.11. “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.

1.6.12. “OAT DPO”, “DPO”, or “Data Protection Officer” refers to the trust Data Protection Officer.

1.7. 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 responsible for the data and other inputs you provide to artificial intelligence systems and tools (AI), and for ensuring the outputs you generate are stored, shared, and used in compliance with the provisions of this policy and other OAT policies. OAT provides guidance on the use of AI, which should be read in conjunction with this policy.

2.5. You are responsible for the care and safety of the technology provided, and must take all reasonable steps to avoid damage, faults, or breakages, including 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.

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. The IT Team must be notified, and provide consent, before you attempt to connect, either physically or wirelessly, any personal devices inside any OAT premises (also see section on Use of Personal Devices).

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

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

2.12. You must always lock the screen of your device when leaving it unattended (e.g. computer or mobile phone). This includes very short periods, such as leaving the device unattended to make a drink.

3. Authorised applications

3.1. The authorised system for secure, daily productivity and file storage is Microsoft 365 (e.g. for email, messaging, word-processing, spreadsheets, file storage and collaboration). The use of academy Google accounts, files and applications is permitted until the transition to Microsoft 365 is complete.

3.2. Social media and messaging applications, such as Facebook and Twitter, are used for one-way communication, most commonly to share information about OAT and its academies with parents, carers and the wider community.

3.3. You may use Whatsapp for work-based messaging and communication. However, Whatsapp is an encrypted, private messaging service and is not supported, monitored or controlled by OAT. If you use Whatsapp, you must satisfy each of the following:

3.3.1. You do not share personal information about children or staff in your messages,

3.3.2. The device on which you send and receive messages is compliant with the relevant provisions of this policy,

3.3.3. 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,

3.3.4. You avoid sharing files,

3.3.5. You ensure that the latest software version and updates are installed on your device(s),

3.3.6. Your application is secured with 2FA (instructions are here),

3.3.7. When asked by an Appropriate Person, you provide all messages in the format requested.

3.3.8. Use is at the user's risk; support will not be provided by IT Teams.

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

3.5. The use of unauthorised communication and file sharing applications is acceptable when joining and working with existing external agencies and professional groups (e.g. Zoom, Facetime, Webex, iCloud, Dropbox). In these instances, staff must adhere as closely as possible to the same conditions covering the use of Whatsapp, as well as those in all related OAT policies (e.g. the Data Protection and Freedom of Information policy).

3.6. 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. SIMS, 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. You must not share personal, sensitive, or confidential data with any staff, child, or third party, unless explicit consent has been received from the academy principal, or relevant senior manager in head office.

4.3. You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or without express, written approval from the principal, or OAT Data Protection Officer (DPO).

4.4. You must not search for, view, download, upload or transmit any explicit or inappropriate material when using OAT's internet or device(s), unless required to do so as part of your role **AND** another member of staff is first notified of your intended action.

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. The OAT internet service is provided for work purposes, only. Personal browsing is permitted during breaks only, provided no searches, transactions, messages or online interactions are conducted that might breach this policy, 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 are required to destroy 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. For security, safeguarding and compliance purposes, OAT routinely monitors the use of devices, applications and internet services.

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. Please see Appendix 1 for guidance on what this might mean.

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.

6.3. Email should be used for 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 anonymised.

6.5. You are advised to limit what you write in emails, messages, or electronic data transfers, and ensure you are not sharing earlier message threads containing personal or confidential information.

6.6. All personal data must be protected when sent using email or other unsecure electronic method (e.g. file attachments). The level of security is dependent upon the type of data being protected. A basic level of protection might be one of the following:

6.6.1. to provide the document as a SharePoint or OneDrive link, specifying the level of access for the recipient(s).

6.6.2. password protect the document being shared via email, and send the password to unlock the document via a different means of communication (e.g. mobile phone text message). Sending a password in a second, separate email is **NOT** considered secure.

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. You must only use OAT-owned computers, laptops and other computing devices on academy or OAT head office premises. Personal Devices are permitted for use only where no OAT or academy device is available **and** all conditions in section 8 are satisfied.

7.2. You must only use OAT-owned mobile phone handsets and numbers as your main work mobile phone, unless use of a Personal Device is authorised through the IT Team. If agreed, the use of a personal mobile phone must satisfy **all** conditions set out in section 4.

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

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

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

7.3.3. images or videos of children, staff or parents are only processed for the activities for which consent has been received.

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

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

7.6. You are expected to use the cloud storage provided with your work account. The use of removable USB drives and other storage media is prohibited, unless they are encrypted by the IT Team and have a pass code for access.

7.7. 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.

8. Use of personal devices (BYOD)

Personal device as your main device for work

8.1. You are not permitted to use a personal computer, laptop or tablet, as your main device for work, unless no other device is available. In which case, **each** of the conditions in 8.3 must be satisfied.

8.2. You may use a personal mobile phone as your main device for work, provided **each** of the conditions in 8.3 are satisfied.

8.3. If no academy or OAT-owned computer, laptop or tablet is available, you may use a Personal Device, provided **each** of the following conditions is satisfied. The same conditions must be satisfied if you choose to use your personal mobile phone rather than an OAT or academy phone:

8.3.1. use of the device is authorised by the IT Team.

8.3.2. the device has installed security/management software by the local IT complying with OAT standard device management tools.

8.3.3. the use of passwords complies with the OAT password policy, and the device is kept locked when not in use.

8.3.4. you retain responsibility for supporting and maintaining the device, ensuring it is continually updated with all patches and updates in accordance with guidance given by the manufacturer, the device operating system, and any installed applications.

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

8.3.6. all data on the device is encrypted by complying with the installation of security/management software and settings by the IT Team.

8.3.7. you understand, in the event of theft or loss of the device, or a security breach, the IT Team will initiate a 'factory reset'* of the device.

PLEASE NOTE: A factory reset will <u>permanently</u> delete all data, including personal data, photographs, videos, emails, applications, and settings from your device.

8.4. If one or more of the conditions in section 8.3 is not met at any time, the device will be blocked.

Personal device for home or remote use

8.5. If you do not have access to an OAT-owned device (e.g. home computer, personal mobile phone) when outside OAT premises, you **may** use a Personal Device for home or remote working, provided:

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

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

8.5.3. 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.

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

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

8.5.6. data stored on the device is encrypted.

8.5.7. 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.

Safeguarding, security and support for personal devices

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

8.7. You must not use Personal Devices to contact academy children. **OAT-owned mobile devices must be used on trips and visits.**

8.8. 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.

8.9. You must inform the IT Team immediately if your Personal Device is involved in a data breach or security incident, or if the device, operating system or installed applications appear to have been tampered with through unauthorised activity.

8.10. The IT Team is unable to provide support for Personal Devices. Please ensure you have a sufficient warranty or support agreement in place to cover technical fixes and advice.

9. Social media and online professionalism

9.1. Please also see the Staff Code of Conduct, Child Protection, and Social Media policies.

9.2. When representing OAT or the academy online, you must express neutral opinions and not disclose any information or publish any comments or posts that may breach confidentiality or affect its reputability.

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 “friend requests” from any children or parents over personal social networking sites, unless the person is known outside of their job role. If the latter is the case, the principal, or head office line manager, must be made aware of the relationship.

9.5. The necessary privacy settings must be applied to all social networking sites (e.g. Facebook, Twitter).

9.6. You must not post or upload any images and videos of children, staff or parents on any online website without consent from the individual(s), as set out in the OAT Data Protection and Freedom of Information and OAT Photography and Videos policies.

9.6.1. In line with the above, you must only post images or videos of children, staff or parents for the activities for which consent has been sought.

9.7. You must not give your home address, personal telephone numbers, social networking details or personal email addresses to children or parents – any contact with parents must be via authorised academy or OAT communication channels.

10. Remote working

10.1. You must ensure that only the data necessary for the activity of your work is accessed and processed at home, in remote locations.

10.2. 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.

10.3. You must ensure the safety and security of all OAT hardware and software, including storing hardware in a secure location when not in use, and ensuring password, privacy and security settings are always activated.

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

10.5. You must ensure that data, information, and video calls are not visible or audible to unauthorised persons, including friends and family. It is recommended that you position your screen, so it is not visible to others, as well as use a video background and headset for online calls.

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 senior member of the IT Team if you believe this policy has been breached, either by you, or another person.

12.2. You should provide full details of any suspected breach. If appropriate, please refer to the OAT Whistleblowing policy and/or the OAT Allegations against ataff policy. Information provided will always be held in the strictest confidence.

12.3. You must notify the IT Team if you receive any unsolicited, or suspicious emails or similar communications. If OAT data might have been compromised, this must also be reported to the DPL or DPO for investigation. (if in doubt, please 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 (see section 4).

12.5. Misuse of the IT Service will be investigated, and action taken 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 breach of my employment contract and of the Staff Code of Conduct.

Signed: Date:

Print name:

Appendix 1 Email FAQs

Email Processing Question	Action
What do I do if the email is informal correspondence between staff or external bodies, confirming a meeting, or agreeing something that is not related to documents detailed in the OAT document retention policy	The email should be deleted once processed
I only want to retain the email due to the attachment?	Save the attachment to the appropriate system. This could be a SharePoint site or a specific system such as CPOMS. Once stored, the email can be deleted. Ensure that the attachment is stored in line with the OAT Records Retention Policy.
What do I do if the email contains information that is required for audit trail purposes such as correspondence on contracts or purchases, correspondence pertinent to quality assurance processes or delivery of projects etc.?	Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties. Save the email to the appropriate SharePoint site in line with the OAT Records Retention Policy.
What do I do if I have received an email that I want to keep but am not sure if I am allowed?	Review the OAT Records Retention Policy for guidance. If you are still unsure, please contact your local DPL.
Am I allowed to retain an email longer than the required retention period as it may be required for litigation?	If data is required for longer than the period stated in the OAT Records Retention Policy than you must clearly document why this data is being kept for longer. Data can be retained for as long as necessary, but we need to have a legitimate reason for doing so. Your mailbox is not to be used to store staff performance data or pupil data such as SEN and Safeguarding information. Emails that contain information about pupils that form part of a pupil record must also be stored elsewhere. Please ensure this data is kept in the appropriate system such as SIMS or CPOMS. If in doubt, contact your DPL or the trust's DPO.
Is there a way to manage my mailbox more efficiently?	Keep on top of monitoring your mailbox. Letting emails build up will make it more difficult to manage. You should always ensure data is stored in the appropriate place/system. This will rarely be your mailbox.

Email Processing Question	Action
Why can I not keep all my emails?	The UK General Data Protection Regulation and Data Protection Act 2018 requires organisations to have definite retention periods and to not retain personal data for periods that are longer than necessary. Retaining data for longer than is necessary or legally required means we are non-compliant and opens the trust to a number of risks such as reputational and financial risks. Storing excessive data can also make handling a Subject Access Request very time consuming and difficult.
What sort of things should I not include in an email?	Never write anything in an email that you wouldn't want to be shared with the subject of the email. Data subjects have a right to request all personal data that we hold about them, even if it's something that would be embarrassing for the person who said it or the trust as a whole. Keep emails succinct and professional, and try to refrain from giving personal opinions
What do I do if I download emails and/or attachments using personal devices?	Please see further guidance in section 8
How should I send documents with my emails?	Where possible, send a link to a document. The link should be set so specific people can access and edit the document. Do not rely on 'people in Ormiston Academies Trust', 'recipients of this message' or 'people with existing access' as this may still lead to a data breach in the event the email is sent to the wrong person