Ormiston Academies Trust

Ormiston Chadwick Academy
Technology Acceptable Use Policy (AUP)

Academy workforce agreement

Policy version control

Policy type	Statutory, OAT template mandatory
Author	Les Leese
Approved by	James Miller, May 2020
Release date	May 2020
Next release date	May 2021
Description of changes	▪ Change to workforce from academy staff ▪ 2. updated to include references to using secure email, or other transfer mediums for sharing sensitive data. ▪ 2. Update to include actions required when receiving suspicious communications. ▪ Formatting changes

Contents

1. Introduction

1.1. Whilst our academy promotes the use of technology and understands the positive effects it can have on enhancing students' 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 principal / executive principal so that any necessary further action can be taken.

1.2. This acceptable use agreement is designed to outline the responsibilities of all the workforce which are staff, volunteers, contractors and visitors when using technology (either personal devices or academy devices), both on and off academy premises.

1.3. 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.

1.4. This agreement must be signed by each staff member. 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 formally recall their agreement. Clarifications concerns, or recalls MUST be expressed in writing (e-mail is preferred) to the appropriate person within the academy.

1.5. Any reference to:

1.5.1. "OAT" refers to OAT (Ormiston Academies Trust) Head office and its academies.

1.5.2. "Academy Data" or "Data" relates to data that is owned by OAT.

1.5.3. "Personal Devices" refers to any device that is not owned by OAT.

1.5.4. "Appropriate Person" refers to a staff member who has authority to grant permission for the area concerned.

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

1.6. OAT retains the sole right of possession of any school-owned 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.Using technology on/off any academy premises

Staff:

2.1. will notify an appropriate person if they receive any and all suspicious emails or other communications. In this first instance this appropriate person will be your local technical support team. If it is found that there has been any interaction where OAT data may have been compromised, then this will also need to be reported to the DPL for investigation. (if in doubt please report to both parties)

2.2. will ensure that they follow the requirement set out by GDPR and OAT Policies when processing or storing data.

2.3. understand that OAT may monitor the use of any OAT device and all internet use without additional notice.

2.4. will only use OAT devices for OAT business unless permission has been granted to do so by an appropriate person.

2.5. whilst conducting academy business, will only use the approved email accounts or other forms of communication that have been provided by OAT.

2.6. will not share sensitive data with any student, staff or third parties unless explicit consent has been received from an appropriate person.

2.7. will ensure that any academy data is stored in line with the OAT data protection policy.

2.8. will delete any chain letters, spam and other emails from unknown sources without opening them unless otherwise agreed by an appropriate person.

2.9. will only use the academy provided internet access for personal use during agreed hours.

2.10. will not search for, view, download, upload or transmit any explicit or inappropriate material when using the academy's internet or academy owned device unless required to do so as part of their role.

2.11. will not share academy-related passwords with students, staff or third parties unless explicit permission has been given from an appropriate person to do so.

2.12. will not install any software onto academy ICT systems or devices unless instructed to do so by an appropriate person.

2.13. will inform the ICT Technical Team of any issues with devices such as errors and alerts that may affect the security or function of the device.

2.14. will not remove or disable any software or systems implemented to ensure the security of academy owned devices.

2.15. if permitted will only store academy data on removable media or other technological devices that have been encrypted.

2.16. are required to return any data to an appropriate person or destroyed in line with the data retention policy or when it is no longer required or as port of an exit strategy.

Electronic Data Transfers

2.17. Email is not a confidential means of communication. There is no guarantee that electronic communications will remain private. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Once an email is transmitted it may be altered. Deleting or recalling an email will not eliminate it from computer systems outside of the computer network.

2.18. The burden of responsibility for the appropriate use of email lies with the sender of the message.

2.19. The email account must only be used for Academy Trust business and for personal purposes within reasonable limits which is permitted, provided this does not interfere with the performance of a member of staff's duties. The sending of personal emails must be marked accordingly in the subject field.

2.20. All personal data must be encrypted when sent using email or other unsecure electronic file transfer method. The level of security is dependent upon the type of sensitive data.

2.21. A basic level of security may be to 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. Please note: sending password in a second separate email is NOT considered secure.

2.22. A more advanced level of communication security may be to use a secure encrypted File Transfer Process (FTP) or use the email encryption setting within the email client. i.e. Microsoft Outlook. Information on how to send secure files via FTP or using email client software such as MS Outlook can be provided by the ICT Technical Team.

3.Mobile devices

Staff:

3.1. will only use OAT provided mobile phones for academy business unless otherwise agreed.

3.2. will not use mobile devices to take images or videos of students unless this has been agreed by an appropriate person.

3.3. will not use academy owned mobile devices to send inappropriate messages, images or recordings.

3.4. will ensure that academy-owned mobile devices do not contain any inappropriate or illegal content.

3.5. will not access or connect personal mobile devices to the academy internet or WiFi networks, unless permission has been given by an appropriate person.

3.6. will not use personal or academy-owned mobile devices to call or send any form of SMS to academy students.

3.7. when processing academy data on a personal device, will ensure that the device is encrypted, and the data will be subject to the data retention policy.

3.8. will only process images or videos of students, staff or parents for the activities for which consent has been sought.

3.9. will ensure that any academy data stored on personal mobile devices is encrypted and give permission for an appropriate person to erase and wipe data off their devices if it is lost or as part of exit procedures.

4.Social media and online professionalism

Staff:

4.1. representing the academy online, e.g. through blogging or on academy social media account, will express neutral opinions and will not disclose any confidential information regarding the academy, or any information that may affect its reputability, unless otherwise directed.

4.2. will not use any academy-owned mobile devices to access personal social networking sites, unless permission has been granted by an appropriate person.

4.3. will not communicate with students or parents over personal social networking sites.

4.4. will not accept “friend requests” from any students or parents over personal social networking sites unless the person is known outside of their job role.

4.5. will ensure that they apply the necessary privacy settings to any social networking sites.

4.6. will not publish any comments or posts about the academy on any social networking sites which may affect the academy’s reputation.

4.7. will not post or upload any images and videos of students, staff or parents on any online website without consent from the individual(s) as set out in the “OAT Photography and Videos Policy”.

4.8. in line with the above, will only post images or videos of students, staff or parents for the activities for which consent has been sought.

4.9. will not give their home address, personal telephone numbers, personal mobile telephone numbers, personal social networking details or personal email addresses to students or parents – any contact with parents will be done through authorised academy contact channels.

5.Working at home

Staff:

5.1. will ensure they obtain permission from an Appropriate Person before any academy data is transferred from an academy-owned device to a personal device. The academy data must be encrypted.

5.2. will ensure only data necessary for the activity of their work is accessed and processed at home. The connection to academy computer networks from home and storage of academy data must be encrypted.

5.3. will ensure no unauthorised persons, such as family members or friends, have access any academy data stored or accessed from any personal devices.

6.Training

Staff:

6.1. will ensure they participate in any e-safety or online data protection training offered and will remain up to date with current developments in social media and the Internet as a whole. It is mandatory for all staff to complete the OAT GDPR training before accessing personal data.

6.2. will ensure that they allow an appropriate person to undertake regular audits to identify any areas of need in relation to training.

7. Reporting misuse

Staff:

7.1. believing that any misuse or breach of policy has taken place, will inform an appropriate person providing full details of the believed misuse. If appropriate, please refer to the OAT Whistleblowing Policy. Information provided will always be held in the strictest confidence.

8. Academy Staff agreement

When logging on to the Academy network for the first time you will be presented with an AUP acceptance page. Your acceptance on this page will represent your acceptance of this policy. Future updates to this policy will trigger a fresh AUP notification when you logon.