OUR CO-OPERATIVE ACADEMIES TRUST

Staff - Acceptable Use Policy

Author: Mr N Emery

Adopted: September 2015

Date of Review: September 2016

Guidelines for Staff

Use of Academy computers and mobile devices by members of staff is governed at all times by the following policy. Please read the policy and where there are any questions or concerns refer these to the IT Services Team Leader, Nathan Emery.

All staff have a responsibility to use the Academy's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the Academy's computer system may result in disciplinary action and civil and/or criminal liability.

Please note that use of the Academy network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which staff can use the system but to ensure compliance with the legal responsibilities and safeguard the reputation of the Academy.

Lastly, the Academy recognises that the distinction between computer use at work and at home is increasingly blurred, with many people using their own computers for work based tasks. Staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment within the Academy.

Computer Security and Data Protection

- Staff will be provided with a personal account for accessing the computer system, with an individual username and password. This account will be tailored to the level of access you require and is for your use only. As such, you must not disclose your password to anyone.
- You must not allow a student to have use of a staff account unsupervised and under no circumstances access to SIMS.
- When leaving a computer unattended ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- Where student or staff details and/or assessment information are stored on any portable device the member of staff to whom that belongs must show due diligence and treat the information confidential.
- Portable devices include, but are not limited to, laptops, USB sticks, tablet devices and mobile phones.
- Storage systems, where possible should be encrypted.
- When data is no longer required the member of staff must delete it from any portable device.
- When publishing or transmitting non-sensitive material outside of the Academy staff should take steps to protect the identity of any student.
- Staff are responsible for backing up their own data kept. This includes data stored on USB memory sticks or other devices.
- Staff must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Lost devices will have the remote wipe command (RWC) sent to remove all data, this is supported by most smartphones, Academy devices are setup for RWC, Staff personal are advised to enable RWC.
- Equipment taken offsite is not insured by the Academy. If you take any Academy computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.
- Academy related sensitive and confidential material should only be printed to printers located in staff offices or to the staffroom.

Academy Laptops

- Academy laptops are issued to staff with off-line full administrator rights which gives the user the ability to install software and hardware. Administrator rights can be removed if the user repeatedly installs software that may harm functionality of the equipment.
- When requested by the IT services staff Academy laptops should be returned to Academy within 48 hours of any request.

Personal Use

The Academy recognises that occasional personal use of the Academy's computers is acceptable and is permitted with the following conditions -

- Use must comply with all other conditions of this AUP as they apply to non-personal use, and all other Academy policies regarding staff conduct;
- Use must not interfere in any way with your other duties or those of any other member of staff;
- Use must not have any undue effect on the performance of the computer system; and
- Use must not be for any commercial purpose or gain unless explicitly authorised by the Academy.

Personal use is permitted at the discretion of the Academy and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by the site team or IT services staff, and must not be used until approved. This test must be performed at regular intervals as required by Academy's normal rules on electrical safety testing.
- Staff must not connect personal computer equipment to Academy networked computers without prior approval from the IT Services, with the exception of storage devices such as USB memory sticks.
- USB memory sticks must be regularly checked to ensure that they do not have viruses or malware that could damage the Academy network.

Conduct

- When using the Academy staff must act in a professional, safe, legal and business appropriate manner and in accordance with the Academy's dignity at work policy. Unacceptable uses includes:
  - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
  - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- Staff must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- Staff must not intentionally damage, disable, or otherwise harm the operation of computers.
- Staff should endeavour to use resources efficiently. Examples include:
  - Excessive downloading of material from the Internet;
  - Excessive storage of unnecessary files on the network storage areas;
  - Use of computer printers to produce class sets of materials.
- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

- Please refer to "Guidance for safer working practice" and "Guidance on Social Networking".

Communication with Students

Staff must:

- Ensure that personal social networking sites are set at private and students are never listed as approved contacts
- Never use or access social networking sites of students.
- Not share personal contact details with students including their mobile telephone numbers.
- Only use equipment provided by the Academy to communicate with children or parents.
- Only make contact with children for professional reasons and in accordance with any Academy/service policy
- Recognise that text messaging should only be used as part of an agreed protocol.
- Not use internet or web-based communication channels to send messages to a child/young person other than those provided by the Academy

Photography and Videos

Staff must:

- Be clear about the purpose of the activity and what will happen to the images when the activity is concluded.
- Be able to justify images of children in their possession and avoid making images in one to one situations or which show a single child with no surrounding context
- Ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.
- Only use equipment provided or authorised by the Academy
- Report any concerns about any inappropriate or intrusive photographs
- Photographs taken must be checked with parents/carers prior to being used for public displays.

Staff must not:

- Display or distribute images of children unless they have consent to do so from parents/carers
- Use images which may cause distress
- Use mobile telephones or any other similar devices to take images of children
- Take images 'in secret', or taking images in situations that may be construed as being secretive.

Further information can be found in the guidance for safer working practice for adults who work with children and young people document.

Use of Email

All Academy staff are provided with an email address for communication both internally and with other email users outside the Academy. The following considerations must be made when communicating by email:

- Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may be made available to third parties.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Staff should check email as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending.
- Staff must not purchase goods or services on behalf of the Academy via e-mail without proper authorisation.
- All Academy emails you send should have a signature containing the sender's name, job title and the name of the Academy.
- E-mail is not a secure method of communication that can be easily copied, forwarded and archived. Unless explicitly authorised to do so staff must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the Academy.
- Having an external email address may lead to receipt of unsolicited email containing offensive and/or sexually explicit content. The Academy will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- Staff must not send chain letters or unsolicited commercial e-mail (also known as SPAM).
- Emails with harmful attachments will be monitored and filtered by IT Services

Supervision of Student Use

- Students should be supervised when using the Academy network.
- Supervising staff are responsible for ensuring that the Acceptable Use Policy for students is enforced.

Privacy

- Use of the Academy computer system including email accounts and storage areas is subject to monitoring by the Academy to ensure compliance with this Acceptable Use Policy and applicable laws. This includes remote monitoring of an interactive logon session. The Academy reserves the right to keep a complete record of sites visited on the internet by both students and staff. Usernames and passwords used are not monitored or recorded.
- Staff should avoid storing sensitive personal information on the Academy computer system that is unrelated to Academy activities (such as personal passwords, photographs, or financial information).
- The Academy may also use measures to audit use of computer systems for performance and diagnostic purposes.
- Use of the Academy computer system indicates your consent to the above described monitoring taking place.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the Academy, as well as other staff or Students.
- Staff are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, music, messages, and other material downloaded or copied. If materials on the Academy computer system or the internet are not marked with the copyright symbol (©) staff should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- Staff must consult a member of the IT Services before placing any order of computer hardware or software, or obtaining and using any software believed to be free.
- All schemes of work and presentations are the intellectual property of OUR Co-operative Academies Trust unless approved for distribution by a Director of Faculty or the Principal.

Reporting Problems with the Computer System

The procedure for reporting faults is as follows:

- Staff should report any problems that need attention to a member of IT Services as soon as is feasible.
- Problems that seriously hinder a task or teaching and require immediate attention should be reported by telephone; any other problem must be reported via email.
- Staff suspecting a computer has been affected by a virus or other malware must report this to a member of the IT Services immediately.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. Staff must immediately inform the IT Services Team Leader, or the Principal, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within the Academy that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by yourself, another member of staff, or a student via the Academy computer system.

Reports should be made either via email, by telephone or in person. All reports will be treated confidentially.

See whistleblowing policy.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

1. "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and Student SEN data. This list is not exhaustive.

When this policy was reviewed, an equality impact assessment was conducted to ensure any changes did not have an adverse effect under the terms of the Equality Act 2010. Should you have any comments regarding this policy, please contact the Academy.