HARRIERS BANBURY ACADEMY

ACCEPTABLE USE POLICY - STAFF

Version control	
Acceptable Use Policy – Staff [2022-09-01]	Reviewed and updated to include guidance re use of Whatsapp
Acceptable Use Policy – Staff [2021-04-23]	Reviewed and updated previous version to align with new DPO appointment.

Date of next review:	**September 2024**	**Owner:**	**Director of HR & Compliance**
Type of policy:	**Trust**	**Approving Body:**	**Executive Operational Board**

ACCEPTABLE USE POLICY

1. Introduction

This policy is based on the Aspirations Academies Trust template Acceptable Use Policy and is intended to promote and ensure the acceptable use of ICT systems and infrastructure by staff, governors and trustees.

The Academy provides a range of ICT resources which are available to staff members, governors and trustees. In order to ensure the safety of staff, governors, trustees and pupils, it is important that all staff members, governors and trustees follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the Academy's ICT systems and infrastructure.
- Define and identify unacceptable use of the Academy's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and Academy devices.
- Specify the consequences of non-compliance.

This policy applies to staff members, governors and trustees. All users of the Academy's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the Academy of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the Academy's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to The Principal.

2. Provision of ICT Systems

All equipment that constitutes the Academy's ICT systems is the sole property of the Academy.

No personal equipment should be connected to or used with the Academy's ICT systems.

Users must not try to install any software on the ICT systems without permission from the Principal. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Principal is responsible for approving the purchase and/or allocation of ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the Academy's computer and network hardware.

3. Network access and security

All users of the ICT systems at the Academy must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the Central IT Team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Academy DP lead as soon as possible.

Users should only access areas of the Academy's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the Academy ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not

compromise the security of the data on the Academy ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

4. Academy Email

Where email is provided, it is for academic and professional use. Personal use is only allowed subject to this being for short periods during recognised break times and the use being compliant with expectations set out in this policy.

The Academy's email system can be accessed from both the Academy computers, and via the internet from any computer. Wherever possible, all Academy related electronic communication must be via the Academy's email system.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, offensive, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the Academy does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official Academy business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.
- Access to the Academy's email system will always take place in accordance with data protection legislation and in line with other relevant policies e.g. confidentiality.
- Members of the community should immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.

- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on Academy headed paper would be.
- Academy email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

5. Internet Access

Internet access is provided for academic and professional use. Personal use is only allowed subject to this being for short periods during recognised break times and the use being compliant with expectations set out in this policy. Priority must always be given to academic and professional use.

The Academy's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Academy DPL/Safeguarding Lead.

Staff must not therefore access from the Academy's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the Academy and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Academy);

- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the Academy may undertake a more detailed investigation in accordance with the Trust's Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

6. Digital cameras

The Academy encourages the use of digital cameras and video equipment, subject to the Photography and Video at School Policy being followed. Staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in Academy only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in Academy is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the Academy network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted.
- Staff are expected to familiarise themselves with the Photography and Video at School Policy

7. File Storage

Staff members are allocated an area on the network and on the Trust-approved Cloud platform (Google Workspace) for their own work as well as access to shared drives. Any Academy related work should be stored in one of these approved areas. Personal files are not permitted on the network or on the cloud platform. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example, copyright music files.

It is also the responsibility of staff to ensure permissions on any files shared in Google workspace is correct i.e., read-only or not downloadable etc

Any files stored on removable media must be stored in accordance with relevant policies of the Academy, including the Information Security Policy and the Electronic Information and Communications Systems Policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No Academy data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or Academy data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

8. Mobile Phones

Mobile phones are permitted in the Academy, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on Academy trips. Where appropriate, the Academy provides equipment for taking photos.
- All phone contact with parents regarding Academy issues will be through the Academy's phones. Personal mobile numbers should not be given to parents.

Use of Whatsapp

WhatsApp is not permitted for use on work issued devices or personal devices for work business. Members of staff are able to use WhatsApp on their own devices for personal communication however, staff should not communicate about any work related matters using their personal WhatsApp accounts. This includes the sharing of any work related information which could include categories of personal data.

9. Social networking

The Academy has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the Academy, staff and students at all times and that they treat colleagues, students and associates of the Academy with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the Academy's reputation, nor the reputation of individuals within the Academy are compromised by inappropriate postings.
- Use of social networking sites for Academy business is not permitted, unless via an officially recognised Academy site and with the permission of the Principal.
- Members of staff will notify the Academy DPL if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the Academy/setting.
- No Academy information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the Academy who are not directly related to the person posting them, should be uploaded to any site other than the Academy's website.
- No comment, images or other material may be posted anywhere, by any method that may bring the Academy or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so, please seek advice from the Principal.

10. Monitoring of the ICT Systems

The Academy may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the Academy's ICT system is, or may be taking place,

or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted.

Monitoring software is installed to ensure that use of the network is regularly checked under the authority of the Principal to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other Academy policy;
- investigate a suspected breach of the law, this policy, or any other Academy policy.

11. Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the Academy's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Principal considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The Academy reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

12. Monitoring

The Academy will monitor the effectiveness of this and all of its policies and procedures and conduct a full review and update as appropriate. Normally this will be on a two year cycle but, where necessary, interim reviews will be undertaken,

The monitoring and review will include looking at how policies and procedures are working in practice to reduce the risks posed to the Academy.

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As an Academy user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the Academy rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the Academy acceptable use policy. If I am in any doubt I will consult with the Academy DP Lead.

I agree to report any misuse of the network to the Academy DPL/Safeguarding Lead. Moreover, I agree to report any websites that are available on the Academy internet that contain inappropriate material to the Safeguarding Lead/Principal. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Principal. .

Specifically, when using Academy devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a school setting or that may cause disruption to the Academy's network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.
I understand that the Academy will monitor communications in order to uphold this policy and to maintain the Academy's network (as set out within this policy).

Signed …… Date ……..

Print name ……