Magna Academy

ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

Version control	
Electronic Information and Communications Systems Policy [2022-09-01]	Reviewed and updated to reflect references to UK GDPR and the use of Whatsapp
Electronic Information and Communications Systems Policy [2021-04-01]	Reviewed and updated previous version to align with new DPO appointment.

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

Electronic Information and Communications Systems Policy

1. Introduction

This policy is based on the Aspirations Academies Trust template Electronic Information and Communications Systems Policy.

The Academy's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the Academy who are required to familiarise themselves and comply with its contents. The Academy reserves the right to amend its content at any time.

This policy outlines the standards that the Academy requires all users of these systems to observe, the circumstances in which the Academy will monitor use of these systems and the action the Academy will take in respect of any breaches of these standards.

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 General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the Academy's Data Protection Policy for further information. The Academy is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the Academy's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Academy's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The Academy has the right to monitor all aspects of its systems, including data which is stored under the Academy's computer systems in compliance with the UK GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets) and voicemail, but it applies equally to the use of fax machines, copiers, and similar equipment.

2. Equipment Security and passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 6 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership team who will liaise with the Regional Technical Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the Academy's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the Academy e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership team and/or the IT Operations/Regional Technical Manager may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the Academy's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of Regional Technical Manager.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The Academy reserves the right to require employees to hand over all Academy data held in computer useable format.

Members of staff who have been issued with a laptop, Chromebook, iPad (or other mobile device tablet), must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g., ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

3. Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the Academy's existing systems, programmes, information or data which could have the effect of harming or exposing to risk or harm the Academy's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Regional Technical Manager] who will consider bona fide requests for work purposes. Please note that this includes instant messaging programmes, screensavers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the Academy's systems. If in doubt, the employee should seek advice from the onsite IT Technician or the Regional Technical Manager or a member of the Senior Leadership Team.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming;

- Instant messaging;
- Chat rooms;
- Social networking sites; and
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to the Academy's systems without the prior approval of the Regional Technical Manager or Senior Leadership Team. This includes, but is not limited to, any telephone, iPad (or other mobile device tablet), USB device, digital camera, MP3 player, infrared connection device or any other device.

The Academy monitors all emails passing through its systems for viruses. Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in '.exe') onsite IT Technicians or the Regional Technical Manager should be informed immediately if a suspected virus is received. The Academy reserves the right to block access to attachments to emails for the purpose of effective use of the system and compliance with this policy. The Academy also reserves the right not to transmit any email message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the Academy's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled '**4. E-mail etiquette and content'** below and '**6.Inappropriate Use of the Academy's Systems'** for guidance.

4. E-mail etiquette and content

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The Academy's e-mail facility is intended to promote effective communication within the business on matters relating to the Academy's business activities and access to the Academy's e-mail facility is provided for work purposes only.

Staff should not use the Academy's email facility for personal emails at any time.

Staff should always consider if email is the appropriate medium for a particular communication. The Academy encourages all members of staff to make direct

contact with individuals rather than communicate by email wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need-to-know basis. The content and language used in the message must be consistent with the Academy's best practice.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to review their draft carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the email to be read out in public or subjected to scrutiny then it should not be sent.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the Academy. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Academy in the same way as the contents of letters or faxes.

E-mail messages will need to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether email is an appropriate form of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The Academy standard disclaimer should always be used on every email.

Staff should ensure that they access their emails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to emails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the email should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via email, you should inform the Director of Business and Operations who will usually seek to resolve the matter informally.

If an informal procedure is unsuccessful, you may pursue the matter formally under the Academy's formal grievance procedure. (Further information is contained in the Academy's Grievance Policy and Procedure.)

As general guidance, staff must not:

Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;

- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private emails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the Academy;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them;
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;

- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service-related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature;

The Academy recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an email which has been wrongly delivered should return it to the sender of the message. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. Academy Data Protection Lead should be informed as soon as reasonably practicable.

5. Use of the web and the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the Academy, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the Academy's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the Academy (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the

Academy's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use Academy systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The Academy's website may be found at magna-aspirations.org. This website is intended to convey the Academy's core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site, and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The Academy should refrain from texting and using systems such as **WhatsApp** for any work related matters using work issued or personal phones. The Academy requires staff to use alternative systems to make contact with staff (such as emails). Please also refer to the **Acceptable Use Policy – Staff** with regards to this matter.

Staff should not use the Academy's systems for personal use.

The Academy reserves the right to restrict or prevent access to certain telephone numbers or internet sites.

6. Inappropriate use of equipment and systems

Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the Academy's Disciplinary Policy and Procedure.

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):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
(b) Transmitting a false and/or defamatory statement about any person or organisation;
(c) Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
(d) Transmitting confidential information about the Academy and any of its staff, students or associated third parties;
(e) Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Academy;
(f) Downloading or disseminating material in breach of copyright;
(g) Copying, downloading, storing or running any software without the express prior authorisation of the Regional Technical Manager
(h) Engaging in online chat rooms, instant messaging, social networking sites and online gambling;
(i) Forwarding electronic chain letters and other materials;
(j) 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 our Disciplinary Policy and Procedure, 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.

7. Monitoring

7. 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.