BRANSTON JUNIOR ACADEMY
ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

Last Updated: 7th Jan 2026

Last update: 3.9b to reflect up-to-date cyber security staff training

1.0 SCOPE

1.1 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.

1.2 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.

1.3 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.

1.4 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 1998 together with the Employment Practices Data Protection Code issued by the Information Commissioner.

1.5 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.

1.6 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.

1.7 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 Data Protection Act 1998.

1.8 This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads, Word Pads, (and other mobile device tablets), iPhones, Blackberries, mobile phones, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

2.0 EQUIPMENT SECURITY AND PASSWORDS

2.1 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.

2.2 If given access to the Academy e-mail system or to the internet, staff are responsible for the security of their terminals.

2.3 Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs, laptops, tablets, Chromebooks and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the IT Subject Leader, the Business Manager, the Deputy Headteacher or the Headteacher.

2.4 On the termination of employment for any reason, staff are required to provide 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.

2.5 Members of staff who have been issued with a laptop, iPad and mobile phone, 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.

2.6 Staff should ensure that their password is known only to them and is not easy to guess (examples of poor/weak passwords include: password, 123456, Welcome 1). There is no precise manner in which passwords should be constructed, but best practise (as discussed on staff meeting with East Midlands Cyber security police officer, Justin Mekkaoui – 14 May 2024) is to use the random 3 words structure; e.g. mountainchairsplendid.

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.

2.7. All members of staff should observe screen locking when away from device even if just for a short period of time. MP, or BT to provide routine reminders of this.

3.0 SYSTEMS USE AND DATA SECURITY

3.1 Members of staff should not delete, destroy or modify any of the Academy's existing systems, programs, 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.

3.2 All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the IT Subject Leader or the Headteacher, (who may seek guidance from the IT Support Team), who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

3.3 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 IT Subject Leader, the Deputy Headteacher or the Headteacher.

3.4 The following must never be accessed from the network because of their potential to introduce viruses and to accidentally reveal or be exposed to content or dialogue that could undermine, or be seen in conflict with, professional conduct:

- instant messaging;
- chat rooms;

- social networking sites; and
- web mail (such as Hotmail or Yahoo)

3.5 No device or equipment should be attached to our systems without the prior approval of the Computing Subject Leader, the Deputy Headteacher or the Headteacher. This includes, but is not limited to, any smart phone, iPad (or other mobile device tablet), USB device, digital camera, MP3 player or any other device.

3.5b Employees of the Academy may use own personal devices to take photos and videos of the children for the purpose of website, Academy social media, and recording of work with the following conditions to be carefully adhered to: Any, and all, images and videos that have been recorded on an employee's (of the Academy) personal device are to be deleted from both the device and cloud storage immediately after use – in this context, 'use' covering the taking of the image/video and any immediate subsequent action, such as uploading onto the Academy's website, or FaceBook page. It is essential to make clear to employees that the images/videos are to be deleted prior to the device leaving the Academy, or the site of residential/visit. Regular reminders will be offered, including via Mr. Thornton's safeguarding reminder of the week within the weekly 'Week Ahead' memo to staff.

Staff are made aware of this requirement/stipulation on an annual basis by the HT and/or computing lead (MP – Dec '22).

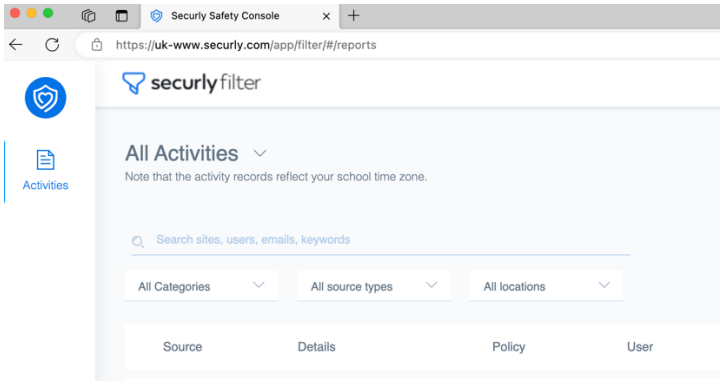
Employees of the Academy will not take photos of children to be published externally without the express parental permission having been given.

3.6 The Academy monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). The Computing Subject Leader, Deputy Headteacher, Business Manager or Headteacher should be informed immediately if a suspected virus is received. They will then contact the IT Support Team (BlueCube as of June 2025). The Academy reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The Academy also reserves the right not to transmit any e-mail message.

3.7 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.

3.8 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 Inappropriate Use of the Academy's Systems and guidance under "E-mail etiquette and content" below.

3.9 February 2024 update. Filtering and monitoring: The Academy's internet traffic is carefully monitored on a daily basis by Mr. Pyburn. We have chosen Securly as our filtering and monitoring system; a key feature of the system is the ability to see internet history of all onsite users. MP (Mr. Pyburn) (and BlueCube, our support partner) have access to an admin portal detailing web history and internet searches, including 'flagged' material from within the previous 30 days:



BT (HT) is DSL for managing online safety, but will work in conjunction with CoG, the governor responsible for computing, and MP (computing lead) for guidance and for keeping abreast of current filtering and monitoring standards and requirements. MP will regularly review the effectiveness of the filtering and monitoring systems in place (as of February 2024: Securly) and will at the review, discuss effectiveness along with (any) necessary enhancements/changes with our support partner (June 2025: BlueCube).

3.9b All staff will receive regular training on Cyber Security. This will be provided (or sourced) by MP and will address current needs and will be regularly updated accordingly, especially if a large turnover of staff. For the academic year 2023-2024, this was provided by PC Justin Mekkaoui (of East Midlands Cyber Security Team) on May 14th, 2024 at a twilight staff meeting. For staff unable to make that meeting, MP will use the materials from that meeting to provide relevant

training. All staff received an update for cyber security training on Monday 5th January 2026 during a whole-staff INSET.

4.0 EMAIL ETIQUETTE AND CONTENT

4.1 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.

4.2 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.

4.3 Staff are permitted to make reasonable personal use of the Academy's e-mail facility provided such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the Academy's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

4.4 Staff should always consider if e-mail 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 e-mail wherever possible to maintain and enhance good working relationships.

4.5 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.

4.6 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 write a draft e-mail first, review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained where appropriate.

4.7 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.

4.8 E-mail messages may of course 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 e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

4.9 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 e-mail.

4.10 Staff should ensure that they access their e-mails at least once every working day and stay in touch by remote access when travelling or working out of the office. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

4.11 All governor-related matters should be communicated to governors through the use of their BJA email addresses. Under no circumstances should sensitive data (e.g., that which is not in the public domain) be communicated outside of the BJA email system, without prior consent of the headteacher.

4.12 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 Group immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

4.13 If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform the Headteacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

4.14 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 Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

4.15 **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 e-mails 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 e-mails to those who do not have a real need to receive them
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals
- 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 e-mail 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
- Email 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

4.16 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.

4.17 Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail 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. Your Line Manager/Head of Department or the Principal should be informed as soon as reasonably practicable.

4.18 **Email retention**: Although the Freedom of Information Act offers no dictate about the period of email retention, the Academy has, in consultation with the Governing body, made a decision to retain emails for six months after the receipt of the email. These emails, which contain GDPR-related data, e.g.; it is possible to identify someone from the information within the email, are to be made available to members of the public as part of a FOI request. After the six month period has passed, the emails can, if appropriate, be deleted from the staff members inbox.

5.0 USE OF THE WEB AND THE INTERNET

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 The Academy's website may be found at www.branstonjunioracademy.co.uk This website is intended to convey our 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 Group in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

6.0 PERSONAL USE OF THE ACADEMY'S SYSTEMS

6.1 The Academy permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

6.2 Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

6.3 The following conditions must be met for personal usage to continue:
(a) use must be minimal and take place substantially out of normal working hours (that is, during the member of staff's usual break time or shortly, before or after normal working hours);
(b) personal e-mails must be labelled "personal" in the subject header;
(c) use must not interfere with business or office commitments;
(d) use must not commit the Academy to any marginal costs;
(e) use must comply at all times with the rules and guidelines set out in this policy;
(f) use must also comply with the Academy's compliment of operational policies and procedures including but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

6.4 Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Any Excessive or inappropriate personal use of the Academy's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

6.5 The Academy reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

7.0 INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

7.1 Reasonable personal use is permissible provided it is in full compliance with the Academy's rules, policies and procedures (including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure).

7.2 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.

7.3 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 Computing Subject Leader, the Deputy Headteacher or the Headteacher

(h) engaging in on line chat rooms, instant messaging, social networking sites and on-line 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.

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

7.5 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.

8.0 USE OF MICROSOFT TEAMS TO SUPPORT DISTANCE AND BLENDED LEARNING

8.1 RECORDING STAFF OR OTHER PUPILS: At BJA, we don't film or take photos of someone without their permission; by respecting their privacy this demonstrates our respectful behaviour towards others. The recording of still images, filmed images or audio of staff or other pupils without their permission, and the distribution of such images, is strictly forbidden.

8.2 CHAT FUNCTIONS: Within BJA, we treat each other with respect through the words we say and how we say them. Likewise within Teams, making inappropriate, offensive or unkind comments (including the use of emojis, GIFs and/or images) will not be tolerated.

8.3 SHARING OF IMAGES: Within our lessons at BJA, we often use images or video clips to show on the board or on paper. They are always appropriate to the learning task. Within Teams, we may use similar files; these visual or audio files shared with others must always be appropriate to the learning task.

8.4 INTERFERENCE WITH OTHERS' WORK: At BJA, our children and staff know not to interfere with other's work. Within Teams, we expect our school members to not interfere with another's work without their permission, whether it is work submitted (such as Word document or photo of their hand-written work) or shared work in a collaboration space (such as in the class OneNote).

8.5 COLLABORTAIVE WORKING: AT BJA, we know the value of sharing and discussing ideas with a partner, a table group, or the whole class. In Teams, there is an expectation that children and staff will try to engage in online collaborative work whilst working in a respectful and helpful manner and making sure that all are following instructions carefully.

Keeping everyone safe at BJA is central to all that we do. We recognise that there are circumstances when children will require and receive additional support during remote learning. We agree that when working 1-1 with a child using the Teams video chat feature, our video camera will be turned off and we will communicate with audio only, supplemented through the use of the Microsoft Whiteboard feature to communicate ideas and concepts visually.

8.6 ACADEMIC HONESTY: In our classrooms at BJA our children know not to copy the work of others. Within Teams when submitting their work children know to agree to their usual standards of honesty and be careful not to plagiarise work and must avoid copying off the internet. We expect our children to be honest in class about their work being their own and the same is true for within Teams

8.7 APPROPRIATE LEARNING ENVIRONMENT: At BJA, our children and staff know how important it is to arrive at school on time and that mobile phones will be kept away from the learning. When using Teams to enhance their learning we will all upkeep a level of appropriate learning environments. This includes: not lying in bed; making sure no music is on in the room; mobile phones are not to be used during the lesson unless directed by the teacher. Many recent computers (from about 2015) have the capability of blurring the background when in a video meeting; this feature should be enabled if available. If not, a plain background can help other members of the video meeting to not become distracted.

8.8 GENERAL BEHAVIOUR DURING LESSONS: Behaviour when working as part of an online lesson should be as expected in line with normal BJA classroom learning for all children and staff: quietly attentive; prepared to ask and answer questions; attempt learning tasks whatever the challenge; engage respectfully with others when collaborating.

8.9 USEAGE EXPECTATIONS: During term time, learning at BJA takes place between 8:45 and 3:30. Regarding access, all staff will make concerted efforts to access the internet so that distance teaching is possible. It is assumed that pupils will do

likewise, but we at BJA appreciate that there may be instances when pupils may have limited access to the internet or to online devices.

We also recognise and respect that everyone has times in the day where it will not be possible to engage in Teams; this includes staff (due to personal reasons such as home-schooling their own children or caring for a relative). Staff are NOT expected to reply to all messages from children and their families, especially those outside of the times that BJA is normally open for learning. Likewise, teachers are encouraged and supported to be flexible in their approach to when they can support their pupils' learning within Teams.