Changes made to the attached policy (November 2024)

1. The policy has been significantly revised and restructured. This work was completed by the Director of IT Services.

2. Consistency has been imposed so that capital letters and hyphenation are more consistent; bullet point lists have been reformatted.

3. A contents page has been added and updated.

4. Inclusive language has been used.

5. Language has been updated to reflect the organisation of the Trust Board (rather than the previous Governing Body). It is also designed to reflect the multi-school nature of an academy trust.

The NSB Trust

Electronic Communication and Information Policy

To be reviewed annually

Contents

1. Introduction

The Trust'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 Trust who are required to familiarise themselves and comply with its contents. The Trust reserves the right to amend its content at any time.

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

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the Trust's Data Protection Policy for further information. The Trust 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 Trust's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Trust's disciplinary procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

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

This policy mainly deals with the use (or misuse) of computer equipment, Email, internet connection, telephones, iPads (and other mobile device tablets), Smart Phones, laptops, Chromebooks, mobile phones and voicemail but it applies equally to the use of fax machines, copiers, scanners, 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 8 characters including numbers, letters and special characters. All passwords should be complex.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Director of Information Services 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 Trust'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 Trust's Email 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 Group and/or the Director of Information Services 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 School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff or a pupil 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 explicit approval of Director or Manager of Information Services.

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 Trust reserves the right to require employees to hand over all Trust data held in computer useable format.

Members of staff who have been issued with a mobile device (laptop or Surface Pro), Smart Phone or any other device (for example a USB stick) 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 device is lost or stolen. Staff should also observe basic safety rules when using such equipment including 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 Trust's existing systems, programs, information or data which could have the effect of harming or exposing to risk of harm the Trust, 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 Director of Information Services 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.

All members of staff need to inform Director or Manager of Information Services before sharing any data with any third parties so the Trust can carry out a Data Protection Impact Assessment (DPIA).

Where consent is given, all files and data should always be virus checked before they are downloaded onto the Trust's systems. If in doubt, the employee should seek advice from the Director of Information Services.

No device or equipment should be attached to our systems without the prior approval of Director of Information Services or Senior Leadership Group. This includes but is not limited to, any Smart Phone or telephone, iPad, laptop (or other mobile device tablet), USB device, i-pod, digital camera, infra-red connection device or any other similar device.

The Trust 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'). The Director of Information Services should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to Email for the purpose of effective use of the system and compliance with this policy. The Trust 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 Trust's computer systems may result in disciplinary action up to and including summary dismissal. Further guidance on what constitutes misuse is contained in the section: Inappropriate Use of the Trust's Systems, and guidance can also be located in the next section.

4. Email etiquette and content

Email 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 Trust's Email facility is intended to promote effective communication within the business on matters relating to the Trust's business activities and access to the Trust's Email facility is provided for work purposes only.

Staff are permitted to make reasonable personal use of the Trust's Email facility provided such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the Trust'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.

Staff should always consider if Email is the appropriate medium for a particular communication. The Trust 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 Email system should be written as professionally as a letter 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 Trust's best practice.

Emails 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 Email first, print it out and review it 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 Emails can be the subject of legal action, for example, in claims for breach of contract, confidentiality, defamation, discrimination, harassment, and similar, against both the member of staff who sent them and the Trust. Staff should take care of the content of Email messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Trust in the same way as the contents of letters.

Email messages may of course be disclosed in legal proceedings in the same way as paper documents. They may also be disclosed as part of dealing with subject access requests when they arise. Deletion from a user's inbox or archives does not mean that an Email is obliterated and all Email 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 forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that Email 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.

During working hours, 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 Human Resources who will usually seek to resolve the matter informally. They will direct you to the relevant policies pertinent to your situation.

If an informal procedure is unsuccessful, you may pursue the matter formally under the Trust's formal grievance procedure.

5. General guidance

Staff must not:

- send any Email, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally
- send any Email 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 Trust
- 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 Email unless the appropriate authority has been obtained. A name typed at the end of an Email 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 Email, 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.

The Trust 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 and delete the email as soon as possible to minimise any further risk to individuals whose data could be breached. 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. The Director of Information Services should be informed as soon as reasonably practicable.

6. Use of 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 for the Trust, 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 access any web page or any files from the Trust's system (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 Trust (whether intending to view the page or not) might be offended by the contents of a page or if the fact that the Trust'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 take extreme care what using the Trust's 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 Email such content to others unless certain that the owner of such works allows this.

The Trust should refrain from texting and using systems such as WhatsApp for Trust related matters using personal phones. The Trust require staff to use alternative systems to make contact with staff (such as emails or MS Teams).

The Trust has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the Trust and may not be reproduced electronically or otherwise for the purpose of passing it to any individual not directly employed by the Trust. Any exceptions to this must be authorised jointly by the Director of Information Services and the Assistant Headteacher with responsibility for line managing IT, who will liaise with the Senior Leadership Group as appropriate and necessary.

6. Personal use of school systems

The Trust permits the incidental use of its internet, Email and telephone systems to send personal Email, browse the web and make personal telephone calls subject to certain conditions set out below.

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.

The following conditions must be met for personal usage to continue:

- 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)
- personal Emails must be labelled "personal" in the subject header
- use must not interfere with business or office commitments
- use must not commit the Trust to any marginal costs
- use must comply at all times with the rules and guidelines set out in this policy
- use must also comply with the Trust's compliment of operational policies and procedures

7. Inappropriate use of equipment and systems

Reasonable personal use is permissible provided it is in full compliance with the Trust's rules, policies and procedures

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

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the Email 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 Trust 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 Trust)
f) downloading or disseminating material in breach of copyright
g) copying, downloading, storing or running any software without the express prior authorisation of Director of Information Services
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 Trust 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.