Electronic Communications Policy

Date Published	**June 2016**
Version	**2**
Last Approved Date	**March 2021**
Review Cycle	**3 Years**
Review Date	**March 2024**

"Learning together; to be the best we can be"

1. Introduction

1.1. This policy addresses the use of electronic communications by employees and will apply to all employees and governors of Nexus Multi Academy Trust, consultants, contractors and agents employed by the Trust and provided with authorised access to the Trust's equipment, systems or information.

1.2. It is every employee's responsibility to:

- read and comply with the requirements of the policy and its appendices.

- report any breaches of this code e.g. misuse of e-mail, Internet, Intranet, telephones etc. either to their Headteacher/line manager or via the Trust's Confidential Reporting Code.

1.3. This policy can be made available in other languages and formats on request.

1.4. Every employee has a duty of care for equipment such as phones and computers that are provided for their use. It is expected that employees will take reasonable steps to maintain the security and safety of equipment. This includes not leaving equipment in view in unattended vehicles and storing it securely when not in use. Mobile phones must be secured by a PIN to prevent unauthorised use if they are lost or stolen, the PIN must not be written down or kept with the phone. The loss, damage or malfunctioning of any computer equipment or data storage device must be reported to the academy or Trust ICT technician.

1.5. Misuse or loss of communications equipment due to negligence will result in employees being requested to reimburse costs to the Trust and may result in disciplinary action.

1.6. Whilst using the Trust's communications technology systems employees should also ensure they comply with the associated Trust policies on Information Governance and Information Security.

2. Electronic Communications and the Law

2.1. The most relevant legislation regulating electronic communications are:

- The General Data Protection Regulation (2018). (relating to the use of personal information);
- The Computer Misuse Act 1990 (relating to unauthorised access and creation or distribution of computer viruses);
- The Copyright Designs and Patents Act 1988 (which relates to unauthorised copying often referred to as software piracy);

2.2. Breach of any of the above can constitute a criminal offence. Where the Trust believes a criminal offence has taken place, it has a duty to inform the Police. Using the Trust's facilities in any way to break the law will be considered as gross misconduct under the Disciplinary Procedure.

3. Content and Usage

3.1. Internet Access is restricted through the use of web filtering software which prohibits the majority of inappropriate or offensive material. The content of emails is also monitored for policy enforcement, messages containing either words or attachments which breach the policy are automatically blocked.

3.2. You should be confident that anything which you access or send meets the following criteria:

- There is a legitimate business need (other than mundane personal use described later)
- That it is within the law and does not breach copyright
- That you have the authority to send the message (i.e. when committing the Trust or academy to a course of action)
- Communications must comply with the Trust's Dignity at Work Policy.
- General advice on e-mail etiquette can be found in Appendix 3. A template for 'Out of Office' messages is supplied in Appendix 4.

4. Home Working

4.1. The rules outlined in this Policy apply to any equipment and systems provided or accessible to you when working from home.

4.2. If you work from home on an occasional basis it is important that you are contactable to the academy and your colleagues. Arrangements should be made with your Headteacher/line manager and communicated with colleagues.

4.3. **COLLEAGUES MUST NOT REVEAL PERSONAL HOME/MOBILE TELEPHONE NUMBERS WITHOUT PRIOR PERMISSION FROM THE HOME WORKER.**

5. Personal Use

5.1. Occasional and reasonable use of the Trust's Electronic Communications systems is permitted providing that:

- It is in your own time i.e. outside normal working hours.
- It does not interfere with work performance or divert you from your duties.
- It is not used for furthering outside business interests or for personal monetary gain.
- The use of the Internet conforms to all other requirements in this policy.
- Usage does not adversely affect the performance of the e-mail system or academy network.

5.2. For the avoidance of doubt employees are advised to not publish anything that may bring themselves or the Trust into disrepute e.g. if you have any inclination that your comment/post may be taken in the wrong way don't say it.

5.3. The only personal usage tolerated is in the following areas:

- Email
- Internet Access
- Social Networking sites, Personal blogs

5.4. Email

5.4.1. A minimal level of mundane personal use is tolerated. This use must be outside your working time. Be aware that emails are monitored and that personally sensitive information should not be sent. Messages should not contain anything that others may find offensive or distasteful. Examples of material that is not permitted are those with a sexual content, jokes or chain letters, a more comprehensive list is detailed in Appendix 1. Personal encryption of messages is prohibited.

5.4.2. If you receive messages which breach this policy then you should do the following:

- If you know the sender, reply advising them that Trust Policy prohibits that type of message and ask them not to send any more similar messages.
- If the message is from another Trust employee then contact your Headteacher/Line Manager for further advice.
- If you are offended or upset by the message you should refer to the Dignity at Work Policy and discuss it with your Headteacher/Line Manager.
- If the message is from outside the Trust and you do not know the sender then advise the academy/Trust ICT technician who can arrange to have messages from specified senders blocked.

5.4.3. Such material may for example not be identifiable until the e-mail is opened and in these cases, employees will not be held responsible provided that they report it immediately. These items should never be passed on to other Trust or non-Trust individuals.

5.5. Mobile Phones

5.5.1. Mobile phones should not be used during the school day, unless in an emergency, and should be kept in a secure place on silent or turned off during lesson time. Staff are permitted to use their mobile phones during break times

5.6. Internet Access

5.6.1. Limited personal use is tolerated outside of working time. Although every attempt is made to prevent access to unsuitable sites it is your responsibility not to access any sites containing unsuitable material (some examples are listed in Appendix 2). Be aware that all internet access is routinely monitored and logged and sites containing unsuitable material are prohibited at all times. The downloading of information for personal use is not permitted at any time.

5.6.2. All internet connections should be via the Trust's network.

5.7. Social Networking Websites, Personal Blogs etc

5.7.1. Social networking websites, blogs (personal diary accounts) and other such communication methods are useful tools for:

- promoting Trust services and the activity of the academy
- accessing professional networks/information
- communicating with hard to reach groups e.g. young people, community groups etc.
- publicising events and news stories

5.7.2. Social networking sites are those which contain personal information about the respective individual and where social interaction between different parties takes place. These sites are very popular and whilst we cannot be prescriptive about what you do in your own time out of work, it is necessary for us to outline what we consider would be detrimental behaviour or written content on a site that could potentially lead to disciplinary action being taken against you.

5.7.3. This section of the Electronic Communications Policy applies to the content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT equipment.

5.8. Cautionary advice – Personal Use on Personal Equipment

5.8.1. The Internet and its social networking sites, blogs (personal diary accounts), message boards, forums and content sharing sites are open to all to view, therefore, for your own safety and protection, caution must be exercised when using such sites.

5.8.2. Anything that you publish, particularly personal information e.g. date of birth, address, photographs etc may be used by others either for illegal or nuisance purposes e.g. identity theft, spam e-mails.

5.8.3. Where you identify yourself as working in a public facing role that could be deemed contentious, such information could also give rise to unwanted attention from service users.

5.8.4. Any illegal activity which is posted on the Internet in an open forum, can also be viewed by the Police or other government agencies.

5.8.5. Employees of the Trust are ambassadors for the Trust and our academies and should be aware that any serious misconduct or criminal offences committed during or outside working hours which could bring the Trust into disrepute may result in disciplinary action being considered.

5.8.6. Personal opinions should not be stated in blogs relating to official business. If a personal blog clearly identifies that you work for The Trust (including the academy), and you express any idea or opinion, then you should add a disclaimer such as "these are my own personal views and not those of Nexus Multi Academy Trust". Please note that this does not preclude the Trust from taking action in cases it considers misconduct.

5.9. Guidelines for use of social networking sites and blogs

5.9.1. The Trust recognises that social media is now an important business tool and that tools such as Twitter are important sources of information and to create professional networks.

5.9.2. A small group of Trust employees represent the Trust and/or an academy on Twitter and Facebook. Other employees should not create posts on social media purporting to represent official Trust opinion.

5.9.3. The following applies to employees who are either provided with access to social networking sites, blogs or other such communications tools for work purposes or use of such tools in an employee's personal time using Trust or personal equipment.

5.9.4. Employees must not:

- Reveal confidential information about the Trust in online postings. This might include revealing information relating to the Trust's children and young people, business plans, policies, employees, governors, contractors, financial information or internal discussions. This list is not exhaustive and you should think carefully before making any postings. Please consult your Headteacher/line manager if you are unclear about what might be deemed confidential.

- Criticise or embarrass the Trust, its children, young people and families or employees in a public forum (including any website), whether in jest or otherwise. You should respect the reputation of the Trust and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague you should raise the matter via your Headteacher/line manager using the correct channels e.g. Dignity at Work Policy or Grievance Procedure. If you have a concern or criticism about the Trust and its practices you should raise this via your Headteacher/line manager or the Confidential Reporting Code.

- Post comments that may be derogatory or defamatory towards colleagues, senior leaders, governors, children, young people and/or their families or contractors or may be deemed to be intimidatory or constitute harassment, whether in jest or otherwise. This list is not exhaustive and you should think carefully before making any postings.

- Use bad language, innuendo, discriminatory statements etc. that could potentially bring the Trust into disrepute.

- Publish film or photographs on the Internet of activity that may bring the Trust in to disrepute.

- Publish photographs of children or vulnerable adults on the Internet (without prior consent) in breach of safeguarding legislation.

- "follow" members of the public using a Trust account as this could be misconstrued.

5.10. Request Process

5.10.1. In order for employees to establish social media accounts for work purposes they must first seek the approval of the Headteacher who will in turn discuss the request with the Chief Executive Officer.

5.11. Unacceptable Use

5.11.1. The accessing or distribution of offensive, illegal or unsuitable material is unacceptable and subject to disciplinary action and/or prosecution.

5.11.2. Offensive material is anything which is abusive, intimidating, malicious or insulting. The persistent abuse of power, or the belittling of someone, either in public or private, which makes them feel upset, threatened, humiliated, vulnerable or undermines their self-confidence, through the use of Information Technology is unacceptable and will be deemed to be bullying or harassment. The Trust's Dignity at Work Policy gives a list of examples of what constitutes bullying and harassment. In the specific context of electronic communications please see Appendix 1 for examples.

5.11.3. Employees must not engage in:

- Posting information that may tend to disparage, threaten, or harass others on the basis of gender, race, age, disability, religion or belief, sexual orientation or national origin;
- Excessive personal use of the internet and social networking sites on Trust or personal equipment during working time;
- Posting statements that are defamatory or information that is false or misleading concerning the Trust or other organisations and their services/products;

- Distributing confidential or sensitive information about the Trust or its children and young people that might compromise its confidentiality;
- Deliberately using email in such a way that it constitutes bullying or harassment;
- Originating or participating in email chain letters;
- Substantial personal use of email, including the transmission of large documents or programs which will add an unnecessary burden to the network;
- Sending jokes, games and other non-work related emails, in a "chatty" and informal style could lead to problems for both the Trust and its employees – do not assume others share your sense of humour.
- Sending or receiving inappropriate material via e-mail (either within an e-mail or as an attachment) such as adult material (pornography), racism / hate, drugs, terrorist and violent activities, gambling, share dealing, paedophilia etc (unless specifically for work purposes).
- Receiving, archiving, storing, distributing, editing or recording sexually explicit material or materials of a disturbing nature using the Trust's network or computing resources (Appendix 1 provides examples of what would be considered inappropriate materials)
- The use of Internet based email accounts i.e. Hotmail is prohibited unless a case for access has been approved.

5.11.4. The list above gives examples of the types of behaviour which constitute violation of the policy. This is not an exhaustive list and there may be other violations which are not listed here.

5.12. Misuse

5.12.1. Where misuse has been identified, employees need to be aware that disciplinary action will be taken. The following, although not an exhaustive listing, is an example of actions, which would warrant serious disciplinary action with possible suspension/dismissal and in certain cases potentially criminal prosecution:

- Employees accessing certain websites e.g. child pornography and terrorist sites for non-work purposes.

- Employees accessing and/or distributing materials of an unsuitable nature (please refer to Appendix 1 & Appendix 2) via e-mail or within an e-mail attachment.

- Defacement of the Trust/academy website.

- Any involvement in 'hacking', virus propagation and spamming of the Trust/academy or any website or contravention of The Computer Misuse Act 1990.

6. Security arrangements and controls

6.1. Security incidents, including the following examples, must be reported to your academy Headteacher/line manager immediately:

- Where it is believed another person is using an employee's ID/ password. Attempts to log on as another user will result in cancellation of e-mail and Internet access and may result in disciplinary proceedings. Internet passwords should not be disclosed to anyone else. Each Internet user is totally accountable and responsible for usage on his / her account: this is also applicable where users have one "log on" password that gives access to both Internet and e-mail.

- If an employee believes another user is accessing prohibited material.

- Construction of personal / business [non-Trust] websites.

- The settings of the PC anti-virus software being amended or disabled.

- Employees engaging in 'hacking' activities into non-Trust web-sites (serious disciplinary action may result).

- If an employee accidentally accesses a prohibited site – this should be reported to the Line Manager as soon as possible after the incident and details of the incident should be logged.

6.2. Unauthorised devices e.g. i-pods, cameras, non-Trust memory sticks, external hard drives should not be connected to Trust computers as this poses a risk to the security of the Trust's network.

6.3. Any suspicious e-mails or attachments should not be opened or forwarded to others as they may contain a virus.

6.4. When using telephones, either landlines or mobile handsets, and whether for personal calls or in the course of your duties, you should take into consideration the location where you are making the call, whether or not it will distract colleagues and whether or not the nature of the telephone conversation is appropriate in front of colleagues and/or visitors to the Trust/academy. It is also important to be courteous and take into consideration that colleagues may not want to be interrupted by your telephone conversations.

6.5. Personal mobile phones should not be used during working hours unless necessary and should be kept on silent/vibrate when in the office.

Appendix 1 – Offensive and Unsuitable Material

The following identifies the type of content considered inappropriate:

- Aggression including threats or violence, abuse or obscenities
- Material which promotes illegal acts
- Sexual advances, propositions, suggestive remarks
- Sexually explicit or pornographic material
- Discrimination of any kind including insults or "jokes" which are related to a person's sex, sexuality, religion or belief
- Racist abuse including "jokes", insults or taunts
- Offensive abuse, ridicule, "jokes" or name calling relating to a person's disability
- Material which the person knows, or ought to have known, would offend a colleague with particular sensitivities, even if it is not explicitly offensive, e.g. religious views or beliefs, gender identity, sexual orientation etc

This is not an exhaustive list. There may be other material which is not listed here which is offensive or illegal.

In general terms messages should not be sent that are likely to cause offence to other employees or bring the reputation of the Trust into disrepute.

Appendix 2 – Unsuitable Websites

Unsuitable Websites

Certain websites cannot be accessed as a filter controls the access to the majority of unsuitable sites; examples of such sites are detailed below along with other examples of unacceptable use:

- Accessing, displaying, downloading or disseminating threatening, obscene or pornographic material including sites that display full or partial nudity or depict/ graphically describe/display sexual acts, activity or content etc.
- Racism/Hate.
- Militancy & Extremist.
- Drugs - sites that promote or provide information about the use of prohibited drugs (unless for work related purposes).
- Terrorist/violence/weapons.
- Gambling.
- Internet auctions.
- Games – downloadable entertainment or games, or playing games over the Internet.
- Hacking - sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases.
- Share dealing.
- Paedophilia .
- Downloading files, software or videos from the Internet or e-mail system unless there is a business related use for the material i.e. software that may enable a Web page to be viewed correctly.
- Downloading, using or distributing copyrighted material without proper authorisation.
- Construction of personal / business [non-Trust] websites.
- Sending and requesting 'junk mail', fund raising requests or chain letters are banned.
- Saving data to Internet files [known as 'X' files] is not allowed.

Appendix 3: Checklist of Do's and Don'ts

Checklist of Do's and Don'ts

Usage of electronic communications is monitored and filtered to make sure that the facilities are not misused. Limited personal internet use is allowed outside normal working hours. All e-mail messages are recorded and management may, under certain circumstances, monitor specific usage and have access to mailboxes.

Access to web-site material containing adult material, racism/hate, drugs, gambling, terrorist activities, share dealing or paedophilia is banned at all times. Non-business sites such as entertainment, sport and travel should be limited to reasonable access during non-working hours i.e. lunch-time. Please note that attempts to access blocked web sites is also monitored.

WHERE MISUSE IS IDENTIFIED, DISCIPLINARY ACTION WILL BE TAKEN UP TO AND INCLUDING DISMISSAL.

MISUSE OF THE INTERNET, E-MAIL, TELECOMMUNICATION OR COMPUTER EQUIPMENT CAN CONSTITUTE A CRIMINAL OFFENCE.

WHERE THE TRUST BELIEVES A CRIMINAL OFFENCE HAS TAKEN PLACE, IT HAS A DUTY TO INFORM THE POLICE.

Electronic Mail (E-mail)): Do's and Don'ts

DO

- Keep messages short, clear and to the point
- Ensure comments are accurate, justified and suitably worded
- Use file compression software for large attachments – and ensure the recipient has the facility to open them
- Check your mail box regularly and clear unwanted e-mails
- Use folders to store items for efficient retrieval
- Do not store messages unnecessarily either in Outlook folders or in personal folders – delete messages 'past their sell by date' regularly
- Be aware that all emails can be monitored
- Ensure the "out of office" facility is enabled for planned absence – click here for a template message
- Use a Trust recognised email signature format
- Avoid taking paper copies of emails unless for correspondence files or meetings
- Avoid "mail storms" – long discussions sent to a wide distributions list
- Beware of viruses

Appendix 3: Checklist of Do's and Don'ts

- Remember emails have the same legal status as paper mail

DON'T

- Use all capitals, gimmicks such as smiley faces or fancy fonts or 'text speak' – this is very informal
- Open any suspicious emails or attachments
- Reveal your password to anyone else
- Attempt to log on as another user
- Read or send personal emails in normal working hours
- Make excessive personal use of emails
- Put your 'out of office' on whilst working at home
- Send sensitive or emotional messages
- Send an email if it could embarrass the receiver or the Trust
- Send or request 'junk mail', fund raising requests or chain letters
- Reply to SPAM (Slang term for unsolicited mail)
- Send or import software programs by email or any other means unless there is a recognised business need
- Use the urgent flag read receipt too often
- Use the BCC and CC as a political tool when emailing colleagues
- Import screensavers from outside the Trust
- Use inappropriate language or include abusive comments that can be interpreted as threatening harassing or insulting
- Express personal views which may be misinterpreted as those of the Trust
- Distribute or store any material of a sexually explicit image or material of a disturbing nature via email or attached to an email

Appendix 4: Templates

E-mail Out of Office – Template

Standard Out of Office:

"I am currently unavailable until (date). If your enquiry is urgent, please contact (name & contact details)

When unavailable due to meetings:

"I am out of the office until (date/time as applicable). I will respond to your email when I return on (date/time as applicable). If your enquiry cannot wait, please contact (name and contact details)."

E-mail Signature Template

Name
Job title
Academy name
Academy address
Academy contact number
Academy web address