St Dunstan's EDUCATION GROUP

P15 related document – Electronic information and communications systems

Policy Owner: Chief Operating Officer

ISSR Reference: 7h e-Safety Policy

Reviewed: Michaelmas 2024

Approved: Finance and resource committee - Michaelmas 2024

Next Review: Michaelmas 2025

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Annual review	Chief Operating Officer	Michaelmas 2024	Transfer to new template Change to become Group-level policy Additional section added on email monitoring

Contents

1. Introduction and aims

St Dunstan's Education Group (the Group) aims to:

- Use electronic information systems and equipment to promote effective communication and working practices throughout the business
- Ensure that all staff, as users of these systems and equipment, understand how the Group will monitor use of these systems and the action the Group will take in respect of any breaches of these standards
- Monitor all aspects of its electronic information communication systems to ensure they used appropriately, and the necessary controls are in place to protect against harm or unauthorized access, disclosure, use, alteration or disruption.

This Electronic Information and Communication Systems 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, who are required to familiarise themselves and comply with its contents. The Group reserves the right to amend its content at any time. To protect the Group's electronic systems from unauthorised access or harm, all staff are required to always comply with the provisions set out in this policy. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Group's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

This policy mainly deals with the use (or misuse) of computer equipment, email, internet connection, telephones, laptops, mobile devices and voicemail, but equally applies to the use of fax machines, copiers, scanners, and the like.

2. Legislation

This policy is based on advice from Judicium, and informed by the following legislation:

- UK General Data Protection Regulation, (UKGDPR) 2018
- Data Protection Act, 2018
- Regulation of Investigatory Powers Act 2000
- Telecommunication (Lawful Business Practice & Interception of Communications) Regulations 2000.

Use by staff and monitoring by the Group of its electronic information systems is likely to involve the processing of personal data and is therefore regulated by the UK General Data Protection Regulation (GDPR) and all data protection laws and guidance in force. Staff are referred to the Group's Data Protection Policy for further information. The Group is 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 UK law by the Human Rights Act 1988.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

The governing body has ultimate responsibility for ensuring that the Group's electronic information and communication systems and equipment promote effective and compliant communication and working practice but will delegate day-to-day responsibility to the Head of St Dunstan's Education Group. The governing body has a duty to:

- Ensure an approved Electronic Information and Communication Systems Policy is in place and reviewed annually
- Monitor the application of the Electronic Information and Communication Systems Policy, including consideration of annual audits.

3.2 The Head of St Dunstan's Education Group

The Head of St Dunstan's Education Group (the Head of the Group) is responsible for:

- Day-to-day oversight of all electronic information and communication systems matters
- Delegating responsibilities to other competent members of staff.

3.3 The Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Ensuring that the Electronic Information and Communication Systems Policy, and associated policies, are reviewed no less than annually
- Ensuring that a training needs analysis is carried out to ensure that all staff fully understand this policy and that relevant staff members are trained in relevant areas
- Line management of the Director of Digital Services
- Overseeing the implementation of the associated Data Protection Policy and acting as the internal Data Protection Officer
- Reporting on electronic information systems matters to the governing body.

3.4 Director of Digital Services

The Director of Digital Services is responsible for:

- Monitoring each school's compliance with this policy and related policies and procedures
- Conducting an annual review of each school's management of electronic information and communication systems
- Authorising requests to download, install or run software from external sources
- Acting as the functional lead for any cyber-related critical incident
- Line management of the Digital Services team.

3.5 Staff

All staff are responsible for:

- Using the electronic information and communication systems in accordance with this policy
- Adhering to the Staff Acceptable Use Agreement (Appendix A)
- Taking responsibility for the security of the equipment allocated to, or used by them, including not allowing it to be used by anyone, other than in accordance with this policy
- Not downloading, installing, or running software from external sources without obtaining prior written permission from the Director of Digital Services
- Completing mandatory data protection and cybersecurity training every three year. This training will include:
    - Useful insights into the type of cyber-attacks and real-world scenarios
    - Who the threat actors are in cybersecurity incidents
    - Tips and techniques to assist users to keep themselves and the Group's IT systems and data safe
    - The opportunity to discuss good practice with fellow users and the Digital Services team.
- Seeking advice from the Digital Services in the following circumstances:
    - If seeking to attach personal devices or equipment to the network
    - If seeking to download, install or run software from external sources
    - When unclear on appropriate use of the Group's Information and Communication Systems.

3.6 Pupils and parents/carers

Pupils and parents /carers are responsible for:

- Adhering to the Pupil Acceptable Use Agreement (see individual school ICT policies)
- Seeking advice from COO if they have any concerns that this policy is not being followed.

4. Equipment security and passwords

4.1 Passwords

Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Head of the Group or the COO, who will liaise with Digital Services as appropriate. Any employee who discloses their password to another employee in the absence of express authorisation will be liable to disciplinary action in accordance with the Group'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.

Further information regarding Group's password management is detailed in the Information Security Policy, Section 6.

4.2 Logging out

If given access to the Group's email systems, or to the internet, users are responsible for the security of their terminals. Users must lock their terminals when leaving unattended to prevent unauthorised users accessing the system in their absence. If a staff member fails to lock their computer and leaves their terminal unattended, they may be held responsible for another user's activities on their terminal which is in breach of this policy, the Group's Data Protection Policy and / or the requirement for confidentiality in respect of certain information. Leadership Teams and the Digital Services team may complete spot checks to ensure compliance with this requirement.

Logging out prevents others accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that they were not the party responsible.

4.3 Mobile device security

Members of staff who have been issued with a laptop, tablet, mobile phone (or other mobile device), must ensure that it is kept secure at all times, especially when travelling. To ensure that data is protected in the event of the device being lost or stolen, passwords must be used to secure access to data held on such equipment.

Staff should also observe basic safety rules when using the 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.

4.4 Interference with digital infrastructure

Desktop PCs and cabling for telephones or computer equipment must not be moved or tampered with, without first consulting and obtaining the express approval of a member of the Digital Services team.

4.5 Termination of employment

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 Group reserves the right to require employees to hand over all Group data held in computer usable format.

5. System use and data security

5.1 Monitoring and filtering

The following systems are in place to enable the Group to monitor and filter web content and emails.

Web Filter	
Rosemead Preparatory School & Nursery	Cloud Flare
St Dunstan's College	Net Sweeper
Monitoring software for pupil devices	
Rosemead Preparatory School & Nursery	Bark
St Dunstan's College	Senso
Anti-Virus Software	
Rosemead Preparatory School & Nursery	Microsoft Defender
St Dunstan's College	Bit Defender GravityZone
Third party email spam filter	
Rosemead Preparatory School & Nursery	Microsoft 365 Advanced Threat Protection
St Dunstan's College	Microsoft 365 Advanced Threat Protection

These systems are provided to the Group by third-party companies who also ensure the usability, uptime and availability of these systems. Any person that logs onto a device and joins a school network will pick up the filtering and monitoring system for the school the device is being used at.

5.2 Systems, programs, information and data

In order to protect the integrity of the Group's systems, programs, information and data, users must not:

- Delete, destroy or modify any of the Group's existing systems, programs, information or data, which could have the effect of harming or exposing to risk or harm the Group, an individual school, its staff, pupils, or any other party.
- Download, instal, or run software from external sources without obtaining prior written permission from the Director of Digital Services. This includes instant messaging programs, 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 Group's systems. If in doubt, the member of staff should seek advice from the Director of Digital Services.
- Attach devices or equipment to the Group's systems without the prior approval of the Director of Digital Services. This includes, but is not limited to, any personal mobile device or laptop, USB device, digital camera, MP3 player, infra-red connection device, or any other device.
- Open emails from unknown sources or where for any other reason an email appears suspicious (such as attachments ending in .exe). The Group monitors all email passing through its systems for viruses, malware, spoofing and phishing attempts. Users should be cautious when opening emails from unknown external sources or where for any other reason an email appears suspicious (such as attachments ending in .exe). Digital Services should be informed immediately if a suspected virus is received. The Group 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 Group also reserves the right to not transfer any e-mail message.
- Attempt to gain access to restricted areas of the network, or to any password-protected information, unless they are specifically authorised to do so.

6. Email and instant messaging use, etiquette and content

Email and instant messaging are vital business tools, but often lapse inappropriately into an informal means of communication. Email and instant messaging must be used with great care and discipline.

The Group's email and instant messaging facilities are intended to promote effective communication within the business on matters relating to the Group's business activities and access to the Group's email and instant messaging facilities are provided for work purposes only. Staff are permitted to make occasional personal use of the Group's email facility, provided that such use is in strict accordance with this policy (see Section Seven: Personal Use).

6.1 Email etiquette

Users should consider if email or instant messaging is the appropriate medium for a particular communication. The Group encourages all members of staff to make direct contact with individuals rather than communicate by email or instant message wherever possible to maintain and enhance good working relationships.

Messages sent on the email system should be written as professional as a letter 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 Group and the relevant school's best practice.

Emails and instant messaging must 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 message first and review carefully before finalising and sending. If a member of staff would not be happy for the message to be read out in public or subjected to scrutiny, then it should not be sent.

Staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they must not be forwarded and must be reported to a member of the Executive Team immediately. If a recipient asks a sender to stop sending them personal messages, then this must happen immediately. Where appropriate, the sender of the message should be referred to this policy and asked to stop sending such material.

Emails and instant messages can be the subject of legal action, for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc. against both the individual who sent them, an individual school or the Group. Incorrect or improper statements can give rise to personal liability of staff and to liability of the Group in the same way as the contents of the letters. Messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean the message is obliterated. All messages should be treated as potentially retrievable, either from the main server or using specialist software. Users should assume that messages may be read by others, and not include them in anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Staff should ensure that they access their emails at least once every working day. Out of office responses must be used if emails will not be accessed for more than one day. Staff should endeavour to respond to emails marked 'high priority' as soon as is reasonably practicable.

If a staff member feels that they have been harassed or bullied or offended by the material sent to them by a colleague via email instant message, they should contact the Chief People Officer (CPO) who will seek to resolve the matter informally. Staff should refer to the Equal Opportunities and

Diversity Policy and the Anti-Harassment and Bullying Policy and the Grievance Policy and Procedures.

6.2 General guidance of use of information and communication systems

As general guidance, staff must **not**:

- Send any email or instant message, internally or externally, containing sexually explicit or otherwise offensive material. This includes resending or forwarding email or instant messages sent by others
- Send any email communication which may be regarded as harassing or insulting. Complaints or concerns about the performance or service of other individuals must be done face-to-face in accordance with normal and courteous practice
- Send or forward private emails to work which they would not want a third party to read
- Send or forward chain mail, junk mail, cartoons, jokes, or gossip, internally or externally
- Contribute to system congestion by sending trivial messages, or unnecessarily copying or forwarding emails to those that 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
- Participate in any internet chat room, post messages on internet chat boards or set up or log text or information, even in their own time
- Download or email content on the internet that may be covered by copyright.

6.3 Websites and the intranet

The Group's individual school websites are intended to convey the Group's and the individual schools' core values and excellence in the education sector. Staff are encouraged to give feedback concerning the websites to the Director of Admissions, Communications and Marketing. Only expressed authorised and designated staff are permitted to make changes to the website.

The individual schools' intranets should be regarded as confidential to the Group and must not be reproduced electronically or otherwise for the purpose of passing it to any individual not directly employed by the Group. Any exception to this must be authorised jointly by the Head of the relevant school and the COO.

7. Personal use of the Group's systems

The Group's email and instant messaging facilities are provided for work purposes only. The Group dissuades personal use of its IT systems, email, internet and telephone systems but understand that it

is not always practical to do so. Therefore, the occasional use of its website, email and telephone systems to browse a website, send personal email, and make personal telephone calls is permitted, subject to the conditions set out below. The Group's policy on personal use is a privilege, not a right. It is dependent upon it not being abused or overused. The Group reserves the right to withdraw permission or amend the scope of this policy at any time. This includes preventing or restricting access to certain telephone or internet sites if the Group considers that personal use is excessive or otherwise in breach of this policy. 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 break times or shortly before or after normal working hours)
- Personal email must be labelled 'personal' in the subject header
- Use must not interfere with business or office commitments
- Use must not commit the Group to any marginal costs
- Use must comply with the rules and guidelines set out in this policy
- Use must also comply with the Group's and individual school's operational policies and procedures including, but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and the Code of Conduct.

Any personal use of the systems may also be monitored and where breaches of this policy are found, action may be taken under the Disciplinary Policy and Procedure. Excessive or inappropriate use of the email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal.

8. Inappropriate use of equipment and systems

8.1 Examples of inappropriate or misuse of equipment and systems

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 Group'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):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist, or other inappropriate or unlawful materials
- Transmitting a false and / or defamatory statement about any person or organisation

- Sending, receiving, downloading, displaying or disseminating material which is discriminatory, offensive or derogatory, or may cause offence and embarrassment, or harass others
- Transmitting confidential information about the Group, any of the schools, or any of its staff, pupils or associated third parties
- Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or the Group)
- Downloading and disseminating material in breach of copyright
- Copying, downloading, storing or running any software without the express prior written authorisation of the Director of Digital Services
- Engaging in online chat rooms, instant messaging, social networking sites and online gambling
- Forwarding electronic chain letters and other materials
- Accessing, downloading, storing, transmitting, or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal. Where evidence of misuse is found, the Group may undertake a more detailed investigation in accordance with the Group's Disciplinary Policy and Procedures, 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.

8.2 Monitoring of usage

We may monitor the email and instant messaging systems or network for the following reasons:

- To determine whether they are communications relevant to work activities
- If the individual is absent from work, to check communications to ensure the continued running of the relevant school
- To record transactions
- Where we suspect that the individual is sending or receiving messages that are:
    - Detrimental to the Group or individual school
    - In breach of the individual's contract or this policy
    - In breach of data protection rights
    - To monitor staff conduct
    - To investigate complaints, grievances or criminal offences.

When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply, we will look at the sender or recipient of the email and the subject heading only and avoid opening emails marked 'Private' or 'Personal'.

The Group does not as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of systems and networks, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon us. To achieve these objectives, we carry out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for and / or accessed by individuals.

We will only intercept (i.e. open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our business and where necessary:

- To determine whether the message is relevant to the carrying on of our business
- To establish the existence of facts
- To check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, i.e. to detect unauthorised use of the system
- To check whether staff using the system in the course of their duties are achieving the standards required of them
- For the purpose of investigating or detecting the unauthorised use of the system
- For the purpose of preventing or detecting crime
- For the effective operation of the telecommunication system.

The content of emails will be examined only in exceptional circumstances, initially by the Director of Digital Services. Information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of individual roles. Information will usually only be shared in this way where the Group believes there may have been a breach of the individual's contract or this policy.

9. Monitoring

This Electronic Information and Communications Systems policy will be reviewed by the COO annually. At every review, the policy will be approved by the Finance and Resources Committee.

10. Links with other policies

This Electronic Information and Communication Systems policy links to the following policies:

- Bring Your Own Device
- Data Breach
- Data Retention
- Information Security
- IT Policy (school-level)
- Privacy notice for governors and volunteers
- Privacy notice for job applicants
- Privacy notice for pupils and parents
- Privacy notice for staff
- Privacy notice for visitors and contactors
- Safeguarding and Child Protection

Appendix A: Staff Acceptable Use Agreement

These rules are designed to protect staff from online safety incidents and promote a safe e-learning environment for pupils:

- I will only use the Group's internet, email, computers, laptops and mobile technologies for professional purposes as required by my professional role.
- I will not disclose my password to anyone.
- When accessing electronic information systems or any other sensitive information relating to the Group, I will ensure that it is conducted on a device that has the appropriate security measures (anti-virus, firewall, encryption) and that I lock the screen when away from the device.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send College business emails using only my school email address and not my personal email address, wherever possible using MySchoolPortal or iSAMS for parent communications.
- I will ensure that any data that I store is stored within the Group' systems on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with the Group policy with consent of the parent or carer. Images will not be distributed outside of the Group without the permission of the parent/carer, pupil and the Head of the relevant school.
- If I bring my own device into one of the schools, it will only be used during non-contact time (without pupils).
- I will report any online safety concerns to the DSL immediately using MyConcern or CPOMS whenever possible, or if MyConcern or CPOMS is not available, I will communicate in person or via email with the DSL.
- My personal mobile phone will be out of sight and switched to silent whenever in the presence of pupils and will only be used for time-bound activities such as taking registers on iTeacher. Personal mobile phones will never be used in the presence of EYFS pupils.
- I will ensure that my online activity, both in and outside of work, will not bring my professional role into disrepute.
- I will support each school's ICT policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will follow the Staff Guidance on Interaction with Students (P1) with respect to electronic communications with pupils and parents.

Confirmation received through the annual staff training acknowledgement form.