P15 IT (Information Technology Policy)

St Dunstan's College

This policy and procedure applies to employees of St Dunstan's Trustee Limited on behalf of St Dunstan's Education Foundation & College Hire Limited.

The IT Policy consists of the following two documents

1. Electronic Information and Communications Systems Policy
2. Information Security Policy

---

1. Electronic Information Systems Policy

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

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

The use by staff and monitoring by the Foundation of its electronic information systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.

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

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

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

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 at least one of each of both upper and lower case letters, numbers and special characters (symbols).

Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Head or Chief Operating Officer (COO) who will liaise with the Digital 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 Foundation'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 Foundation e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to lock their computer when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The College Leadership Team and/or the Director of Digital Services may do spot checks from time to time to ensure compliance with this requirement.

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

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

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of Digital 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 Foundation reserves the right to require employees to hand over all Foundation data held in computer useable format.

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. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

Systems Use and Data Security

The following systems are in place to enable the Foundation to monitor and filter web content and emails:

1) Web Screen is the Foundation's web filter.
2) Microsoft Defender is the Foundation's PC anti-virus.
3) Microsoft 365 Advanced Threat Protection is the Foundation's third-party email spam filter.

These systems are provided to the Foundation by third party companies, who also ensure the usability, uptime and availability of these systems. Any person that logs on to a Foundation device, should pick up these filtering and monitoring systems.

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

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Director of Digital Services who will liaise with the COO to 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.

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

No device or equipment should be attached to our systems without the prior approval of the Director of Digital Services and Chief Operating Officer. 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.

The Foundation monitors all e-mails passing through its systems for viruses, malware, spoofing and phishing attempts. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as attachments ending in '.exe'). Digital Services should be informed immediately if a suspected virus is received. The Foundation 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 Foundation also reserves the right not to transmit any e-mail 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 Foundation'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 Foundation's Systems and guidance under "E-mail etiquette and content" below.

E-mail and Instant Messaging etiquette and content

E-mail and instant messaging (IM) are vital business tools, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The Foundation's e-mail and IM facilities are intended to promote effective communication within the business on matters relating to the Foundation's business activities and access to the Foundation's e-mail and IM facilities are provided for work purposes only.

Staff are permitted to make occasional personal use of the Foundation'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 Foundation'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 e-mail or IM is the appropriate medium for a particular communication. The Foundation encourages all members of staff to make direct contact with individuals rather than communicate by e-mail or IM wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally 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 Foundation's best practice.

E-mails and IMs 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 message first and review it carefully before finalising and sending. As a rule of thumb 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.

All members of staff should remember that e-mails and IMs 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 Foundation. Staff should take care with the content of messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Foundation in the same way as the contents of letters.

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 or IM is obliterated, and all 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 or IM is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that messages may be read by others and not include in 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 e-mails 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 e-mails 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 Executive Team immediately. If a recipient asks you to stop sending them personal messages, then always stop immediately. Where appropriate, the sender of the message 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 e-mail or IM, you should inform the CPO who will usually seek to resolve the matter informally. You should refer to the Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the Foundation's formal grievance procedure. Further information is contained in the Foundation's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.

As general guidance, staff must not:

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

- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice.
- Send or forward private 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 Foundation.
- 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. The message board in the Common Room should be used for these purposes.

- 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.
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service-related issues. Urgent or important messages to family and friends are permitted but must be of a serious nature.

The Foundation 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 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. The COO should be informed as soon as reasonably practicable.

Use of the web and the internet

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

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

As a general rule, if any person within the Foundation (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the Foundation's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

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

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

The Foundation's website may be found at www.stdunstans.org.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 Director of Marketing & Communications in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The Foundation has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the Foundation and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the Foundation. Any exceptions to this must be authorised jointly by the COO and Head.

Personal use of the Foundation's systems

The Foundation dissuades the use of its IT systems, email, internet and telephone systems etc. but understands that it is not always practical to not do so. Therefore. the occasional use of its internet, e-mail, and telephone systems to send personal e-mail, browse the web and make personal telephone calls for personal reasons is permitted, 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:

(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 Foundation 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 Foundation'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.

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. Excessive or inappropriate personal use of the Foundation'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.

The Foundation 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

Inappropriate use of equipment and systems

Occasional personal use is permissible, as above, provided it is in full compliance with the Foundation'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).

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 Foundation's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials.
(b) Transmitting a false and/or defamatory statement about any person or organisation.
(c) Sending, receiving, downloading displaying, or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others.
(d) Transmitting confidential information about the Foundation 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 Foundation.
(f) Downloading or disseminating material in breach of copyright.
(g) Copying, downloading, storing, or running any software without the express prior authorisation of the COO and/or the Director of Digital 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 Foundation 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.

2) Information Security Policy

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Foundation is dedicated to ensuring the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the Foundation to achieve this, including to:

- protect against potential breaches of confidentiality.
- ensure that all information assets and IT facilities are protected against damage, loss or misuse.
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the Foundation of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the Foundation's Data Protection Policy, Data Breach Policy and Electronic Information Systems Policy for further information. These policies are also designed to protect personal data and can be found on the Foundation's shared drives or obtained from the College Office.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, USB drives and smartphones.

Scope

The information covered by this policy includes all written, spoken, and electronic information held, used or transmitted by or on behalf of the Foundation, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Foundation's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Foundation and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the Foundation's Data Protection Policy and Record of Processing Activities. All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss the appropriate security arrangements for the type of information they access in the course of their work with Digital Services, access to sensitive data will need to be approved by the COO or Head.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by Digital Services or by such third party/parties as the Director of Digital Services or COO may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with Director of Digital Services, unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the COO, who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Physical security and procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets and other storage systems with locks shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of the Foundation.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the COO , as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The Foundation carries out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The Foundation has a security entrance system to minimise the risk of unauthorised people from entering the Foundation premises.

CCTV Cameras are in use at the Foundation. Further information can be found in the CCTV policy.

Visitors are required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Computers and IT

Responsibilities of the Director of Digital Services

The Director of Digital Services shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Foundation's security requirements.
b) ensuring that IT Security standards within the Foundation are effectively implemented and regularly reviewed, working in consultation with the Foundation's management, and reporting the outcome of such reviews to the Foundation's management.
c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

Furthermore, the Director of Digital Services shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy.
b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems.
c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements.
d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Chief Operating Officer.
e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff.
f) monitoring all IT security within the Foundation and taking all necessary action to implement this policy and any changes made to this policy in the future; and

g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

All members of staff shall undergo compulsory Cybersecurity training led by the Director of Digital Services. The content of which includes:

- Useful insights into the type of cyber-attacks that may present itself to the users.
- Who the threat actors are in cybersecurity incidents.
- Real world scenarios of cyber-attacks.
- Tips and techniques to assist in users keeping themselves and the Foundations computer systems and data safe.
- The opportunity to discuss "good practice" with fellow users and the Digital Services department.

You must immediately inform the COO of any security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to Digital Services immediately.

You are not entitled to install any software of your own without the approval of the Director of Digital Services. Any software belonging to you must be approved by the Director of Digital Services and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Software can only be installed by Digital Services; you must not attempt to install any software yourself. Requests for software installation should be made to the Director of Digital Services via the Helpdesk.

The use of removeable media (USB drives) etc. is discouraged within the Foundation and we provide secure cloud storage which can be audited and recovered in the event of data loss. There are rare exemptions to this, such as where invigilators use USB drives to securely transfer exam materials from computers or transferring print files to CNC/3D print machines. Regardless, removable media should not be used for the storage or transferal of Foundation documents.

If you detect any virus this must be reported immediately to Digital Services (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access security

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.

The Foundation has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Foundation's network. The Foundation also teaches individuals about e-safety to ensure staff and pupils are aware of how to protect the Foundation's network and themselves. A separate IT and Computing Policy is in place to cover this in more detail for pupils.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by Digital Services. Biometric log-in methods can only be used if approved by Digital Services.

All passwords must, where the software, computer, or device allows:

a) Be at least 8 characters long consisting of at least 3 of the following: both upper- and lower-case letter, numbers and special characters (including spaces).
b) Be changed on a regular basis and at least every term (x3 per year).
c) Not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.).
d) Use second/multi factor authentication methods where possible.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Foundation Executive Team who will liaise with the Director of Digital Services as appropriate. 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 Foundation'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 you forget your password, you should notify the Service Desk to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the Foundation, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

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

Data security

Personal data sent over the Foundation network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Director of Digital 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. Where consent is given all files and data should always be virus checked before they are downloaded onto the Foundation's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the Foundation's Wi-Fi provided that you follow the relevant requirements and instructions governing this use. All usage of your own device(s) whilst connected to the Foundation's network or any other part of the IT Systems is subject to all relevant Foundation Policies (including, but not limited to, this policy). The COO and Head may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by Digital Services.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the Foundation or otherwise without prior written approval of the COO. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the Foundation's computer networks in order for it to be backed up.

Home working

You should not take confidential or other information home without prior permission of the COO or Head and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
b) all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

Communications, transfer, internet and email use

When using the Foundation's IT Systems, you are subject to and must comply with the Foundation's Electronic Information Systems Policy.

The Foundation works to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the COO.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the Foundation cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular, you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Foundation.

Personal or confidential information should not be removed from the Foundation without prior permission from the COO or Head except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) not transported in see-through or other un-secured bags or cases.
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Reporting security breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the COO. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the COO shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the COO. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the COO.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the COO.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.

Related Policies

Staff should refer to the following policies that are related to this information security policy:

- Electronic Information Systems Policy
- Data Breach policy
- Data protection Policy

P15 - IT			
Author/s:	Judicium Saffron Hutt Jon Hanson	**Date Reviewed:**	Michaelmas 2023
Date Ratified:	Michaelmas 2023	**Next Review Date:**	Michaelmas 2024
Committee:	Education Committee	**Clerk to the Governors** **Signature:**	David Richards