Information Security Policy

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 UK General Data Protection Regulation (UK 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 committed to ensuring the security of all information that it holds and implements the highest standards of information security in order to achieve this. This documents 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 unauthorized access, use, disclosure, disruption, modification or destruction.

Staff are referred to the Foundation's Data Protection Policy, Data Breach Policy and Electronic Information and Communication 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 Foundation 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, memory sticks 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 any 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 the IT Manager, access to sensitive data will need to approved by the Chief Operating Officer (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 the IT Manager or by such third party/parties as the IT Manager or Chief Operating Officer 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 IT Manager, unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Chief Operating Officer, 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 Chief Operating Officer, 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 used at the Foundation and monitored by the IT Manager and House Staff.

Visitors are required to sign in at the reception, accompanied at all times by a member of staff. They should 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 UK GDPR and the Computer Misuse Act 1990.

Furthermore, the IT Manager 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 Data Protection 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.

You must immediately inform the Chief Operating Officer of any and all 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 the Director of 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.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the Director of Digital Services. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media is virus-scanned. IT Manager approval must be obtained prior to the transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the Director of 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 everyone is aware of how to protect the Foundation's network and themselves.

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 the Digital Services. Biometric log-in methods can only be used if approved by the Digital Services.

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

a) be at least 6 characters long including both numbers and letters;
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.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Foundation Leadership Team who will liaise with the Director of 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 you forget your password you should notify the IT Helpdesk 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 Chief Operating Officer and the 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 the Director of 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 Chief Operating Officer. 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 network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day and is done by the Director of Digital Services's team.

Home working

You should not take confidential or other information home without prior permission of the Chief Operating Officer or the 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 and Communication 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 Chief Operating Officer.

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 Chief Operating Officer or the 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 Chief Operating Officer. 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 Chief Operating Officer 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 Chief Operating Officer. 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 Chief Operating Officer.

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

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 and Communication Systems Policy;
- Data Breach policy;
- Data Protection Policy.