St Dunstan's EDUCATION GROUP

# P15 – Information Security Policy

**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<br>Change to become Group-level policy |

## Contents

## 1. Introduction and aims

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

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
- Protect and maintain data protection rights in accordance with UK GDPR
- Ensure the security of all information it holds and implement high standards of information security to achieve it.

This includes:

- Protecting against potential breaches of confidentiality
- Ensuring that all information assets and IT facilities are protected against damage, loss or misuse
- Increasing awareness and understanding across the Group of the requirements of information security and the responsibilities of staff to protect the confidentiality and integrity of the information they handle.

The information covered in this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Group, in whatever media. This includes information held on computer systems, paper records, handheld devices and information transmitted orally. For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile devices that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, USB drives and smartphones.

This Information Security 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. All staff are required to comply with the provisions set out in this policy to protect the Group's electronic systems from unauthorised access or harm. 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.

## 2. Legislation and definitions

### 2.1 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

### 2.2 Definitions

| | |
|---|---|
| Information Security | The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. |

## 3. Roles and responsibilities

### 3.1 St Dunstan's Education Group

The governing body has ultimate responsibility for information security but will delegate day-to-day responsibility to the Head of the Group. The governing body has a duty to:

- Ensure an approved Information Security Policy is in place and reviewed annually
- Monitor the application of the Information Security 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 Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Ensuring that the Information Security 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 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 information security 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
- Ensuring that all IT systems are assessed and deemed suitable for compliance with the Group's security requirements
- Acting as the functional lead for any cyber-related critical incident
- Ensuring that IT security standards across the Group are effectively implemented and regularly reviewed, working in consultation with the Dunstan's Executive Team (DET) and reporting the outcomes of such reviews to the COO
- 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, including, but not limited to, the GDPR and Computer Misue Act 1990.

The Director of Digital Services line manages the Digital Services Team, who are responsible for:

- Assisting staff in understanding and complying with this policy at the individual schools
- Providing all staff with appropriate support and training in IT Security matters and use of IT systems
- Ensuring that staff are granted appropriate levels of access to IT systems, taking into account their job role, responsibilities and other special security requirements
- 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 and informing the COO

- Taking proactive action, where possible, to establish and implement IT security procedures and raise awareness with users
- Monitoring all IT security within the Group and taking all necessary action to implement this policy and any changes made to this policy
- Ensuring that regular backups are taken of all data stored with the IT systems at regular intervals and that such backups are stored at a suitable location offsite.

**3.5 Staff**

Staff are responsible for:

- Complying with all relevant parts of this policy at all times when using the Group's IT systems
- Ensuring that computers and other electronic devices are locked when not in use to minimise accidental loss or disclosure
- Informing 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
- Ensuring that passwords are kept secure, changing a password immediately if it is thought that it could have been compromised
- Informing Digital Services of any technical problems (including, but not limited to, possible password breaches, hardware failures and software errors) which may occur on the IT systems
- Informing Digital Services immediately of any virus detected, including if the anti-virus software automatically fixes the problem
- Completing mandatory cybersecurity training, led by the Director of Digital Services, every three years. This training will include:
    - Useful insights into the types of cyber-attack 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 clarification on the security requirements for the types of information they access in the course of their work
    - If seeking to attach personal devices, removable media 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:

- Committing to the Pupil Acceptable Use Agreement
- Seeking advice from COO if they have any concerns that this policy is not being followed.

## 4. General principles

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

All data stored on IT systems and as paper records should be available only to 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 must be installed, maintained, serviced, repaired, and upgraded by the Digital Services team and / or by such third parties as the Director of Digital Services authorises.

## 5. Physical security and procedures

### 5.1 Site security

The physical security of buildings and storage systems will be reviewed on a regular basis. If occupants find security to be insufficient, they must inform the Director of Estates and Commercial Activities, or the COO as soon as possible.

At each school there are regular checks of buildings and storage systems to ensure they are maintained to a high standard and a security entrance system is used at all schools to minimise the risk of unauthorised individuals entering the premises. Visitors are required to sign in at the reception, be accompanied at all times by a member of staff and must never be left alone in areas where they could have access to confidential information.

CCTV is used across the schools' sites. Further information can be found in the individual schools' CCTV policies.

### 5.2 Storage of paper documents

Paper records and documents containing personal information, sensitive personal information and confidential information must be positioned in a way to avoid them being viewed by people passing as much as possible, e.g. through windows. At the end of the working day, or when users leave their desks unoccupied, all paper documents must be locked away to avoid unauthorised access. Available storage rooms, locked cabinets and other storage systems with locks can be used to store paper records when not in use.

Paper documents containing confidential personal information must not be left on office and classroom desks, on staff room tables, or pinned to noticeboards where there is general access, unless there is a legal reason to do so and / or relevant consents have been obtained. Particular care should be taken if documents have to be taken offsite.

## 6. 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 Group has a secure firewall and anti-virus software in place. These prevent unauthorised access and protect the Group's networks. The Group also trains all staff and pupils in e-safety so that they can understand how to protect the Group's networks themselves. A separate ICT Policy is in place to cover this in more detail for pupils at each of the schools.

All IT systems, in particular mobile devices, must be protected with a secure password or passcode, or such form of secure log-in system as approved by Digital Services. Biometric log-in methods are not currently used by the Group or implemented on Group-managed devices. All passwords, where the software, computer, or device allows, must:

- Be at least twelve characters long and have at least one of each of the following: upper and lower-case letter, number and special characters (including spaces)
- Not be obvious or easily guessed (e.g. birthdays, memorable names, events, places etc.)
- Use second / multi factor authentication where possible.

In accordance with the National Cybersecurity Centre's (NCSC) advice on the password burden, the Group does not require regular password changes, however, all users must change their password whenever requested, or there is the possibility that it has been compromised.

With regard to password security, all staff must:

- Keep their passwords confidential
- Not make their passwords available to anyone else unless requested by the Director of Digital Services
- Notify their school's Digital Services helpdesk if they forget their password, or think it may have been compromised.

Any member of staff who discloses their password to another employee in the absence of express authorisation will be liable to disciplinary action under the Group's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's passwords will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

Staff members should avoid writing passwords down whenever possible. If necessary, users may write passwords down provided that they are stored 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 electronic devices with display and user input devices (e.g. mouse, keyboard, touchscreen etc.) must be protected with a screen lock that will activate after a period inactivity. Users must not change this time period or disable the lock.

All mobile devices provided by the Group will be set to lock, sleep or similar, after a period of inactivity, requiring a password, passcode or other form of log-in to unlock. Users must not change this time period or disable the lock.

Staff members 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 when in breach of this policy, the Group's Data Protection Policy and / or the requirement for confidentiality in respect of certain information.

## 7. Data Security

Personal data sent over the Group's networks must be encrypted or otherwise secured. Staff are prohibited from downloading software from external sources without obtaining prior authorisation from the Director of Digital Services, who will consider bona fide requests for work purposes. This includes, instant messaging programs, screensavers, photos, video clips, games, music files and opening any documents or communications from unknown sources. Where consent is given by the Director of Digital Services, all files and data should always be virus checked before they are downloaded onto the Group's systems.

Users may connect their own devices (including, but not limited to, laptops, tablets and smartphones) to the Group's wi-fi networks, provided that they follow the relevant requirements and instructions governing this use. All usage of users' own devices whilst connected to the Group's networks, or any other part of the IT systems, is subject to all

relevant Group and school policies. The Director of Digital Services, the COO or Head of the school may request the immediate disconnection of any such device without notice.

## 8. Home working

Staff must not take hard copies of confidential or other information home without prior permission of the Head of the Group, COO or Head of the relevant school, and should only do so when they are satisfied that appropriate technical and practical measures are in place to maintain the continued security and confidentiality of information. When permission has been given to take confidential or other information home, employees must ensure that:

- Information is kept in a secure and locked environment where it cannot be accessed by other occupants or visitors
- All confidential material that requires disposal is shredded, or in the case of electronic material, securely destroyed as soon as any requirement for its retention has passed.

## 9. Communication, transfer, internet and email use

When using the Group's IT systems, users are subject to and must comply with the Group's Electronic Information and Communication Systems Policy. The Group seeks to ensure that the systems robustly protect pupils and staff and are reviewed and updated regularly.

There are restrictions on international transfers of personal data and transfers to international organisations. Staff may only transfer personal data outside the UK or to any international organisation, with the prior written authorisation of the DPO, as detailed in the Data Protection Policy.

If staff, pupils or other users discover unsuitable sites or any material which could be considered unsuitable, this should be reported immediately to their school's Designated Safeguarding Lead (DSL), the COO, or the Director of Digital Services.

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 Group cannot accept liability for the material accessed or its consequences.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or recorded delivery. Users must not send such information by fax unless they can be sure it will not be inappropriately intercepted. Postal, DX, fax, telephone numbers and email addresses should be checked and verified before information is sent to them. In particular, users must take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

Staff must maintain confidentiality when speaking in public places and mark confidential information 'confidential' and circulate this information only to those that need to know the information in the course of their work for the Group.

Personal or confidential information should not be removed from the premises without prior permission from the Head of the Group, COO, Head of the relevant school, or the Director of Digital Services. When such permission is given, staff must take all reasonable steps to ensure the integrity of the information, and that confidentiality is maintained. Staff must ensure that the information is:

- Not transported in transparent or unsecured bags or cases
- Not read in public places, e.g. waiting rooms, cafes, trains
- Not left unattended or in a place where it is a risk e.g. car boots, cafes, luggage compartments.

## 10. Reporting security breaches

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

When receiving notification of a breach, the COO will immediately assess the issue, including but not limited to, the level of risk associated with the issue and take all steps necessary to respond to the matter. This will include seeking the support of the Data Protection Officer. All IT Security breaches will be fully documented.

Under no circumstances may staff attempt to resolve an IT security breach on their own without first contacting 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 Director of Digital Services and 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.

Full details of how to report data breaches is set out in the individual schools' Data Breach Policy.

## 11. Monitoring

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

## 12. Links with other policies

This Information Security Policy links to the following policies:

- Clear desk policy
- Data breach policy
- Data retention policy
- Electronic information and communication systems policy
- IT policy (school level)