ODBST Information Security Policy

ODBST Level 1 Statutory Policy:	**ALL** Schools require this policy with **no changes** allowed to core text. No changes are necessary to personalise this with school name and branding, as this is a Trust level policy for use, without change, by all schools, **except** where a school contact is required as identified in the content of the policy. LGBs will **note** adoption in LGB meetings. Review will take place at Trust level, and schools will be notified of updates and review dates as necessary.
Other related ODBST policies and procedures:	Data Protection Policy E safety policy Data Breach Policy Cyber Security Policy Freedom of Information Policy
Committee responsible:	FRAPP
Approved by:	FRAPP and Trust Board
Date Approved:	24/06/2025
Review Date:	23/06/2027

1. Policy Statement

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 Oxford Diocesan Bucks Schools Trust (ODBST) is dedicated to ensuring the security of all information that ~~it~~ the Trust and its schools hold~~s~~ and implement~~s~~ the highest standards of information security in order to achieve this. This document sets out the measures taken by ODBST and its schools ~~to achieve this~~, including to:-

- To protect against potential breaches of confidentiality;
- To ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- To support our Data Protection Policy in ensuring all staff in both the Trust and its' schools are aware of and comply with UK law and our own procedures applying to the processing of data;
- To increase awareness and understanding of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle and
- **To establish appropriate controls for student use of personal devices and access to educational technology platforms.**

2. Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.
ODBST school staff are referred to the Data Protection Policy, Data Breach Policy and Cyber Security Policy for further information. These policies are also designed to protect personal data and can be found internally on the shared drive or on the school's website.
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**, gaming devices, smartwatches, and any Internet of Things (IoT) devices.** (**Internet of Things (IoT) devices** are physical objects embedded with sensors, software, and other technologies that connect and exchange data with other devices and systems over the internet or other communication networks.)

3. Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School or Trust, 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**,** students (where applicable), 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 to comply with the provisions contained within it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

Students who breach this policy will be subject to the school's behaviour and disciplinary policies. Serious breaches may result in temporary or permanent restrictions on IT access, and in severe cases, may be treated as serious disciplinary matters.

This policy does not form part of any individual's terms and conditions of employment with ODBST 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.

4. 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 ODBST Data Protection Policy and Information Asset Register/Record of Processing Activities(ROPA). All data must be handled appropriately in accordance with its classification.

Special consideration is given to:

- Children's personal data, which requires enhanced protection under UK GDPR
- Special category data relating to students (health, biometric data, etc.)
- Examination data and assessment information
- Behavioural and safeguarding records
- Post-16 student data where different consent requirements may apply

Staff should discuss with [list staff position who will, if in doubt, will speak to the Trust IT Manager] the appropriate security arrangements for the type of information they access in the course of their work.

All data stored within 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.

In secondary schools, student access to data is strictly controlled and limited to:

- Their own personal academic records (where age-appropriate)
- Learning materials and resources specifically assigned to them
- School-approved educational platforms and applications

All IT Systems are to be installed, maintained, serviced, repaired and upgraded by Turn it on (Schools not with Turn It On please replace this) or by such third party/parties as the ODBST 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 The Trust's IT Manager, unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to [POSITION of member of staff at school] 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 via the Jedu website or via phone call (Judicium - full details of the officer can be found in our Data Protection Policy).

5. 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 far 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.

In secondary schools, additional considerations include:

- Securing examination papers and assessment materials
- Protecting student work and coursework from unauthorised access
- Ensuring confidential student information is not visible in areas where older students may have unsupervised access
- Securing areas where sensitive equipment (e.g., servers, networking equipment) is housed

Available [storage rooms, locked cabinets, and other storage systems with locks] shall be used to store paper records when not in use. If you do not feel you have appropriate and/or sufficient storage available to you, you must inform [NAME/POSITION/SBM] as soon as possible.
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 school.

Particular care must be taken in secondary schools where:

- Students may have legitimate access to staff areas during breaks or for sixth form activities
- Student helpers or prefects may assist with administrative tasks
- Parent/carer meetings occur in multi-use spaces

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 [POSITION of person responsible] as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the school to ensure physical security of the building/s and storage systems:

- [The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.]
- [The School has an intercom system to minimise the risk of unauthorised people from entering the school premises.]
- [The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.]
- [CCTV Cameras are in use at the School and monitored by [POSITION]]. Delete if not applicable

- [Visitors should be 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.]
- Secondary schools implement additional security measures for areas containing examination materials and confidential student records
- Student lockers and personal storage areas are regularly monitored for security compliance

6. Computers and IT

6.1. The Trust IT Manager (Change this if not with TIO to own MSP) shall be responsible for the following:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
- ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management and reporting the outcome of such reviews to the School's management;
- 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.
- ensuring age-appropriate internet filtering and monitoring systems are in place and regularly updated.

6.2. Furthermore, the [SBM/Ops/HT etc] shall be responsible for the following:

- assisting all members of staff in understanding and complying with this policy;
- providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- 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;
- 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];
- taking proactive action, where possible, to establish and implement IT security procedures and to raise awareness among members of staff;
- monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- 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 and
- in secondary schools, overseeing student IT access controls and BYOD compliance;
- coordinating with examination bodies regarding IT security requirements for online assessments.
- Overseeing the security of examination systems and data;
- Maintaining an inventory of all approved educational technology platforms and applications;

7. Student use of IT systems

7.1. Schools shall implement appropriate controls for student access to IT systems, including:

Student Account Management:

- All students must be provided with individual login credentials
- Student accounts must be configured with age-appropriate access controls
- Regular review of student access rights and privileges
- Automatic account suspension/deletion upon leaving the school

Internet Access and Filtering:

- Implementation of robust content filtering appropriate to student age groups
- Different filtering levels for different year groups where appropriate
- Regular monitoring and updating of filtering policies
- Safe search enforcement on all search engines
- Blocking of inappropriate social media platforms during school hours (where applicable)

Educational Platform Security:

- Ensuring compliance with children's privacy regulations for all platforms
- Data sharing agreements in place with educational technology providers

Digital Citizenship Education:

- Age-appropriate education on online safety, digital footprints, and cyber security
- Integration of digital citizenship into the curriculum

7.2. Bring your own device (BYOD) policy (secondary schools)

Where secondary schools permit students to bring personal devices, the following requirements apply:

Device Requirements:

- Devices must meet minimum security standards (updated operating system, antivirus where applicable)
- Devices must be registered with the school IT system
- Parental/guardian consent required for students under 16
- Acceptable use agreements signed by students and parents/guardians

Network Access:

- Student personal devices connect to segregated network with limited access
- No access to staff systems or confidential school data
- Network activity monitoring and logging

Security Requirements:

- Screen lock with password/PIN required
- Automatic software updates enabled
- Regular security compliance checks by Managed service provider

Data Protection:

- No school data to be stored on personal devices unless specifically authorised
- Use of approved cloud storage solutions only
- Immediate reporting of lost or stolen devices

Prohibited Activities:

- No photography/video recording without explicit permission
- No access to inappropriate content
- No circumvention of security measures
- No sharing of login credentials

8. 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 [POSITION in school] 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 [POSITION in school] immediately.

Staff working in secondary schools have additional responsibilities:

- Supervising student use of technology and reporting inappropriate use
- Ensuring examination security protocols are followed
- Modelling appropriate digital behaviour for students
- Participating in regular safeguarding and online safety training
- Reporting concerns about student online safety or cyber bullying

You are not permitted to install any software of your own without the approval of the [POSITION in school/Trust]. Any software belonging to you must be approved by the [POSITION in school/Trust] 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 [POSITION in school/Trust]. This permission must clearly state which software you may install and onto which computer(s) or device(s) it may be installed.

Educational software and applications used with students must:

- Comply with UK data protection law
- Have appropriate data sharing agreements in place
- Be regularly reviewed for security vulnerabilities

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 virus scanned. Approval from [NAME/POSITION in school/Trust] must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the [POSITION in school/Trust] (this rule shall apply even where the anti-virus software automatically fixes the problem).

9. **Security**

9.1. 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.

In secondary schools, staff must also:

- Ensure student access is appropriate to their age and role
- Never share staff login credentials with students
- Supervise student use of technology appropriately
- Log out of all systems when students are present
- Secure all devices when in areas accessible to students

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. All School and Trust staff must undertake RPA cyber security training annually to refresh their knowledge on how to best protect 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 ODBST Ops Team and Turn IT On IT Manager.

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

- be at least 6 characters long including both numbers and letters; **(8 characters minimum for secondary school systems with admin access)**
- be changed on a regular basis
- not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.)

For secondary schools:

- Student passwords must meet minimum complexity requirements appropriate to their age
- Multi-factor authentication required for staff access to examination systems
- Regular password strength audits conducted

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the ODBST or school SLT who will liaise with the [POSITION in school/Trust] 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 Trust'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.

Students found sharing passwords or accessing systems with another person's credentials will face disciplinary action in accordance with the school's behaviour policy.

If you forget your password you should notify the [TIO 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 avoid writing down passwords. 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 time period or disable the lock.

Screen lock timing for secondary schools:

- Staff devices: Maximum 5 minutes inactivity
- Student devices: Maximum 5 minutes inactivity
- Devices in examination settings: Maximum 2 minutes inactivity

All mobile devices provided by the School 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 log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

9.2. Examination security

Secondary schools must implement specific security measures for examinations:

Digital Examination Systems:

- Separate, secure network for online examinations
- Lockdown browsers and secure examination software
- Real-time monitoring and logging of examination activity
- Backup systems and contingency procedures
- Compliance with examination board security requirements

Examination Data Protection:

- Encrypted storage of all examination materials and results
- Restricted access to examination data on need-to-know basis
- Secure transmission of examination data to examination boards
- Retention and disposal schedules in accordance with examination board requirements

Security Incidents:

- Immediate reporting of any security breach during examinations
- Isolation of affected systems
- Full investigation and reporting to relevant examination boards
- Implementation of remedial measures

9.3. Data Security

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

Enhanced protections for children's data:

- All children's personal data encrypted in transit
- Regular audits of data access and usage
- Automatic data retention and deletion schedules

- Privacy impact assessments for all new systems processing children's data

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from [POSITION in school] 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 School's systems.

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

10. Electronic Storage of Data

All portable data and in particular personal data should be stored on encrypted drives using methods recommended by [TIO ODBST IT Manager].

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 School or otherwise without prior written approval of the [POSITION/Headteacher]. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up.

All electronic data is backed up everyday through the Microsoft365 platform and Trust backup systems managed by Turn IT On/(List contractor).

11. Homeworking

You should not take confidential or other information home without prior permission of the [POSITION/Headteacher/ Trust] 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:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- 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.

Additional considerations for secondary school staff:

- **Enhanced security vigilance when working with examination materials**
- **Secure disposal procedures for student work and assessments**

12. **Communications, Transfers, Internet and Email Use**

When using the Trust or School's IT Systems you are subject to and must comply with the Electronic Information and Communication Systems Policy.

The School/Trust 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 [POSITION/SBM/HT].

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 Trust 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 School.

Personal or confidential information should not be removed from the School without prior permission from [POSITION/HT] 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:

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

Additional precautions for examination materials:

- Secure transport containers for examination papers
- Immediate reporting of any loss or potential compromise
- Additional insurance requirements where applicable

13. Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the [POSITION in school/Trust who will consult with the Trust IT Manager]. 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 [POSITION in school/Trust] 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 [POSITION Trust IT Manager]. 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 [POSITION Trust IT Manager].

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to [POSITION in school].

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.

14. Incident response and business continuity

Schools must maintain robust incident response capabilities:

Incident Response Team:

- Designated incident response coordinator
- Clear escalation procedures and contact information
- Regular testing of incident response procedures
- Post-incident review and improvement processes

Business Continuity:

- Backup systems for critical educational functions
- Alternative arrangements for examinations during system failures
- Communication plans for parents and students during incidents
- Regular review and testing of continuity plans

Recovery Procedures:

- Documented system recovery procedures
- Data recovery and validation processes
- Lessons learned integration
- Stakeholder communication during recovery

15. Training and Awareness

Comprehensive training programs must be implemented.

Staff Training:

- Annual information security awareness training
- Role-specific training (e.g., examination administrators)
- Regular updates on emerging threats and technologies
- Incident response training and exercises

Student Education:

- **Age-appropriate digital citizenship curriculum**
- **Online safety education integrated across subjects**
- **Peer education and support programs**

Parent and Guardian Engagement:

- **Resources for supporting online safety at home**
- **Clear communication about BYOD requirements**
- **Regular updates on online safety trends and concerns**

16. Related Policies

Staff should refer to the following policies that are related to this Information Security Policy:

- E – Safety Policy
- Data Breach Policy
- Data Protection Policy