ODBST Cyber 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:	ODBST E- Safety Policy ODBST Data Protection Policy
Committee responsible:	FRAPP
Approved by:	FRAPP
Date Approved:	23/9/2025
Review Date:	22/09/2027

1. Policy Statement

Cyber security has been identified as a risk for the Oxford Diocesan Bucks Schools Trust and every employee needs to contribute to ensure data security.

The Trust has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the School and Trust IT systems.

[Julia Payne, Headteacher – usually the GDPR school lead] is responsible for cyber security within the School.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our Data Protection Policy, and E-Safety/ Acceptable Use Policy.

2. Purpose and Scope

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime.

This policy is relevant to all staff.

3. What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- cost;
- confidentiality and data protection;
- potential for regulatory breach;
- reputational damage;
- business interruption;
- structural and financial instability.

4. Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the ODBST to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Trust IT Manager/Corin Brearley can provide further details of other aspects of the School/Trust risk assessment process upon request.

The ODBST have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

5. Technology Solutions

The ODBST have implemented the following technical measures to protect against cyber-crime:

- firewalls;
- anti-virus software;
- anti-spam software;
- auto or real-time updates on our systems and applications;
- URL filtering;
- secure data backup;
- encryption;
- deleting or disabling unused/unnecessary user accounts;
- deleting or disabling unused/unnecessary software;
- using strong passwords; and
- disabling auto-run features.
- two-factor authentication

6. Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.
- **Inline with Academy Trust handbook updates:** Cyber Security (Section 6.15) New Prohibition**: Trusts and their school must not pay cyber ransom demands under any circumstances.** This aligns with National Crime Agency recommendations.

- All staff must:
    - Choose strong passwords (a strong password contains a mixture of characters including numbers or letters and is at least 8 characters long.

- keep passwords secret;
- never reuse a password;
- never allow any other person to access the school's systems using your login details;
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to Julia Payne as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy;
- only access work systems using computers or phones that the School owns or when given specific permission to do so from the Headteacher.
- not install software onto your ODBST computer or phone. All software requests should be made to Julia Payne; and
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

- The Trust considers the following actions to be a misuse of its IT systems or resources:
  - any malicious or illegal action carried out against the ODBST or using the ODBST's systems;
  - accessing inappropriate, adult or illegal content within ODBST premises or using School equipment;
  - excessive personal use of ODBST's IT systems during working hours;
  - removing data or equipment from ODBST premises or systems without permission, or in circumstances prohibited by this policy;
  - using ODBST equipment in a way prohibited by this policy;
  - circumventing technical cyber security measures implemented by the ODBST's IT team; and
  - failing to report a mistake or cyber security breach.

7. Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

- *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.

- *Assessment of the ongoing risk:* To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified.
- *Notification:* To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
- *Evaluation and response:* To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above. The school will refer immediately to the Trust DPO (Judicium) should this occur.

Contact: data services@judicium.com or Tel: 0345 548 7000