Cyber 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.

Introduction

Cyber security has been identified as a risk for the College and every employee needs to contribute to ensure data security.

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

The Chief Operating Officer and the Director of Digital Services are responsible for cyber security.

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, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Electronic Information and Communications Policy and Clear Desk Policy.

Purpose and Scope

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

This policy is relevant to all staff.

Created: Lent 2024
Next Review: Lent 2025

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; and
- Structural and financial instability.

Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for St Dunstan's College 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 Director of Digital Services can provide further details of other aspects of St Dunstan's College's risk assessment process upon request.

St Dunstan's College 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.

Technology Solutions

St Dunstan's College have implemented the following technical measures to protect against cyber-crime:

(i) Firewalls;
(ii) Anti-virus software;
(iii) Anti-spam software;
(iv) Auto or real-time updates on our systems and applications;
(v) URL filtering;
(vi) Secure data backup;

(vii) Encryption;
(viii) Deleting or disabling unused/unnecessary user accounts;
(ix) Deleting or disabling unused/unnecessary software;
(x) Using strong passwords; and
(xi) Disabling auto-run features.

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 St Dunstan's College or any third parties with whom we share data.

- All staff must:
- Choose strong passwords (a strong password contains [list of types of characters, password length etc. as permitted by your IT systems]);
- Keep passwords secret;
- Never reuse a password;
- Never allow any other person to access St Dunstan's College'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 St Dunstan's IT systems;
- Report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the Director of Digital Services or the COO 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 College owns. Staff may only connect personal devices to the visitor Wi-Fi provided;

- Not install software onto your College computer or phone. All software requests should be made to the Director of Digital Services; and
- Avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using St Dunstan's equipment and/or networks.

- St Dunstan's College considers the following actions to be a misuse of its IT systems or resources:

- Any malicious or illegal action carried out against the College or using the College's systems;
- Accessing inappropriate, adult or illegal content within St Dunstan's College premises or using St Dunstan's College's equipment;
- Excessive personal use of IT systems during working hours;
- Removing data or equipment from St Dunstan's College's premises or systems without permission, or in circumstances prohibited by this policy;
- Using St Dunstan's College's equipment in a way prohibited by this policy;
- Circumventing technical cyber security measures implemented by the IT team; and
- Failing to report a mistake or cyber security breach.

Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

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

(ii) *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.

(iii) *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.

(iv) *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, St Dunstan's College will invoke their Data Breach Policy rather than follow the process above.

Related Policies

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

Data Protection Policy
Data Breach Policy
Information Security Policy
Acceptable Use Policy
GDPR – staff guidance for remote working
Electronic Information and Communications Policy
Clear Desk Policy