TOWNLEY

EST 1937

GRAMMAR SCHOOL

CYBER SECURITY POLICY

1. Introduction

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

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

The Data Manager and IT support team are responsible for cyber security within Townley Grammar 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, Acceptable Use Policy and Electronic Information and Communications Policy

2. Purpose and Scope

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

This policy is relevant to all staff, pupils and Trustees.

3. What is Cyber-Crime?

Cyber-crime is 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 – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.
- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements at our school. The risk to confidential information and personal data is the biggest of all threats from cyber-crime.
- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).
- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.

- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services.
- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

4. Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for Townley Grammar School 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 Data Manager can provide further details of other aspects of Townley Grammar School risk assessment process upon request.

Townley Grammar School 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.

4.1 Technology Solutions

Townley Grammar School 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 software and user accounts;

(ix) using strong passwords; and

(x) disabling auto-run features.

5. Controls and Guidance for Staff

All staff must follow the actions related to cyber-crime and cyber security as listed in this policy.

Technology solutions in isolation cannot protect us adequately, so our systems and controls extend to cover the human element of cyber-crime/cyber security risk.

All staff will be provided with training, 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 Townley Grammar School or any third parties with whom we share data.

It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:

- Physically ringfencing the individuals or teams working on a matter;
- Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
- Disposing of confidential documents securely;
- Having a clear desk policy;
- Discouraging staff from reading confidential papers or discussing sensitive matters in public and;
- Informing staff about the risks of leaving their laptops open and unattended.

Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures on other parties with whom we share information.

All staff must:

- Ensure they are familiar with the risks presented by cyber-crime and cyber security attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g. not forwarding chain letters or inappropriate/spam emails to others. We will help you by continually raising awareness of those risks and providing training where necessary.
- Report any concerns they may have.

5.1 Email Security

Protecting email systems is a high priority. Criminals send emails containing malicious links which have led to data theft, scams, and carry malicious software like worms and bugs. Therefore, Townley Grammar School requires all employees to:

• Verify the legitimacy of each email, including the email address and sender name.

• Avoid opening suspicious emails, attachments, and clicking on links.

• Look for any significant grammatical errors.

• Avoid clickbait titles and links.

• Contact the ICT department regarding any suspicious emails.

5.2 Transferring data

Townley Grammar School recognises the security risks of transferring confidential data internally and/or externally. To minimise the chances of data theft, we instruct all employees to:

• Refrain from transferring classified information to employees and outside parties.

• Only transfer confidential data over school networks.

• Obtain the necessary authorisation from Senior Management and the Data Manager.

• Verify the recipient of the information and ensure they have the appropriate security measures in place.

• Adhere to the School data protection and privacy policies.

• When communicating regarding safeguarding, staff will ensure any emails containing files will be sent encrypted. When communicating outside the borough, Egress Web Access will be used to ensure the security of the data.

• Immediately alert the ICT department of any breaches, malicious software, and/or scams.

5.3 Device Security and Passwords

Townley Grammar School advise staff that they should:

- Choose strong passwords;
- keep passwords secret;
- never reuse a password;
- never allow any other person to access Townley Grammar School's systems using your login details;
- Ensure devices are secured and locked when not in use;
- do 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 Townley Grammar School IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the Data Manager 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 Townley Grammar School owns. Staff may only connect personal devices to the visitor Wi-Fi provided;
- do not install software onto your school computer or phone. All software requests should be made to the IT support team;
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks; and

- Ensure devices are regularly updated with the latest security software. School employees are obligated under the equipment loans agreement and acceptable use policy as part of the equipment loan procedure

6. Misuse of IT systems

Townley Grammar School considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against Townley Grammar School or using Townley Grammar School's systems;
- accessing inappropriate, adult or illegal content within School premises or using School equipment;
- excessive personal use of School's IT systems during working hours;
- removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;
- using School equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by Townley Grammar School'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 if we were to identify a potential cyber security breach:

(i) *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies.

(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, Townley Grammar School will invoke their data breach management plan rather than follow out the process above.