ASPIRATIONS

# Magna Academy

# Cyber Security Policy

| Version control | |
|---|---|
| Cyber Security Policy [2022-09-01] | Reviewed and no changes required. |
| Cyber Security Policy (2021-10) | Policy Created based on Aspirations template policy (version Oct 2021) |

| | | | |
|---|---|---|---|
| **Date of next review:** | **September 2024** | **Owner:** | **Principal/ Trust IT Manager** |
| **Type of policy:** | **Trust Template** | **Approved by:** | **Executive Operational Board** |

**CYBER SECURITY POLICY**

## 1. Introduction

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

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

1.4 The Regional Technical Manager is responsible for cyber security within the Academy.

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

1.6 This policy supplements other data management and security policies, namely our [Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy and Electronic Information and Communications Policy].

## 2. Purpose and scope

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

2.2 This policy is relevant to all staff.

## 3. What is cyber-crime?

3.1 Cyber-crime is simply a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks.

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

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

3.3 It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

## 4. Cyber-crime prevention

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

4.2. The Academy 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 to staff.

4.3 Technology solutions

(a) The Academy has a variety of technical measures in place for protection against cyber-crime. They include:

(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.

4.4. Controls and guidance for staff

(a) all staff must follow the policies related to cybercrime and cyber security as listed in the introduction to this policy, see section 1.

(b) 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 Academy or any third parties with whom we share data.

(c) all staff must:

(i) choose strong passwords (the Academy's IT team advises that a strong password contains *[Eight characters long with capital and lower-case letters, numbers and symbols*); Avoid passwords that can be easily guessed e.g. birthdays.

(ii) keep passwords secret;

(iii) never reuse a password; Change every three months

(iv) never allow any other person to access the Academy's systems using your login details;

(v) 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 Academy IT systems;

(vi) report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to *[DPO and Regional Technical 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;

(vii) only access work systems using computers or phones that the Academy owns. Staff may only connect personal devices to the approved Wifi SSID.

(viii) not install software onto your Academy computer or phone. All software requests should be made to [Principal and the Regional Technical Manager]; and

(ix) avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using Academy equipment or networks.

(x) use secure and private networks only when accessing the Academy's network remotely.

(xi) avoid transferring sensitive data to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, please contact IT support for assistance.

(xii) report stolen or damaged equipment as soon as possible

(d) all staff must not misuse IT systems. The Academy considers the following actions to be a misuse of its IT systems or resources:

(i) any malicious or illegal action carried out against the Academy or using the Academy's systems;

(ii) accessing inappropriate, adult or illegal content within Academy premises or using Academy equipment;

(iii) excessive personal use of Academy's IT systems during working hours;

(iv) removing data or equipment from Academy premises or systems without permission, or in circumstances prohibited by this policy;

(v) using Academy equipment in a way prohibited by this policy;

(vi) circumventing technical cyber security measures implemented by the Academy's IT team; and

(vii) failing to report a mistake or cyber security breach.

(ix) downloading suspicious, unauthorised or illegal software on their Academy's devices.

**5. Cyber-crime incident management plan**

5.1. The incident management plan consists of four main stages:

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

(ii) **Assessment of the ongoing risk** to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.

(iii) **Notification** to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents as appropriate.

(iv) **Evaluation and response** to consider any improvements to data security and evaluate future threats to security.

5.2 Where it is apparent that a cyber security incident involves a personal data breach, the Academy will invoke their Data Breach Policy rather than follow out the process in this section 5.