Cyber Security Policy

This document is called:	Cyber Security Policy
It applies to:	All staff at Bolder Academy
Person responsible for its revision:	Headteacher
Status:	Non- Statutory
Published on:	The Academy Website
Approval by:	Governing Board or Delegated Committee
Review frequency:	Every two years or after any security incident.
Date of approval:	Nov 2022
Date of next approval:	Nov 2024

Introduction

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

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.

The Business Manager is responsible for cyber security within the Academy.

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 Communication Policy.

Purpose and Scope

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 to set out an action plan should the Academy fall victim to cyber-crime.

This policy is relevant to all staff.

What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet. 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 the Academy 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 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 for staff.

Technology solutions

(a) The Academy 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 of mobile devices;

(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

(a) all staff must follow the policies related to cyber-crime and cyber security as listed in earlier in this policy.

(b) all staff will be provided with training at induction or 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 (where the software, computer, or device allows):

a) be at least 8 characters long including both numbers and letters and symbols;

b) be changed on a regular basis and at least every 90 days;

c) cannot be the same as the previous 5 passwords you have used;

d) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Headteacher as appropriate and necessary. This is recommended in our IT Policy as well as managed via the IT system.

(ii) keep passwords secret;

(iii) never reuse a password;

(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 the Business 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 guest Wi-Fi provided;

(viii) not install software onto your Academy computer or phone. All software requests should be made to the Business Manager; and

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

(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.

Cyber-Crime / Critical Incident Management

Incident management 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, the Academy will invoke their Data Breach Policy rather than follow out the process above.