Athena Learning Trust

Trust-wide

Cyber Security Procedure

Review
Reviewed on: 31st October 2022
Reviewed by: Board
Review Period: 3 years

ATHENA
LEARNING TRUST

Contents

PART A

1.1. Application

This Athena Learning Trust Cyber Security Procedure applies to the Athena Learning Trust as a whole and to all the schools in the Trust and the Trust Shared Service, in accordance with and pursuant to the Communications Policy of the Athena Learning Trust.

The Athena Learning Trust, including all the schools in the Trust, their Trustees, governors and staff, must abide by this Athena Learning Trust Cyber Security Procedure.

This Procedure is subject to the Trust's Scheme of Delegation for Governance Functions. If there is any ambiguity or conflict then the Scheme of Delegation and any specific alteration or restriction to the Scheme approved by the Board of Trustees takes precedence.

In implementing this procedure, the governing body, Principal and Trust staff must take account of any advice or instruction given to them by the Athena Learning Trust Head of Information Technology (IT), the Athena Learning Trust CEO or Board of Trustees.

If there is any question or doubt about the interpretation or implementation of this Procedure, the Athena Learning Trust Head of IT should be consulted.

1.2. Approval and review

Maintenance of this Procedure is the responsibility of the Athena Learning Trust Head of IT.

This procedure was approved by the Board of Trustees on: 30 October 2022.

This procedure is due for review by: end of July 2024.

1.3. Terminology

The Trust means the Athena Learning Trust (Athena Learning Trust).

- School means a school within the Athena Learning Trust.
- Principal means the Principal or principal of the school.
- CEO means the chief executive officer of the Athena Learning Trust.
- Governors and Trustees includes governors, Trustees, non-governor members of Trust Committees and members of the Trust Panel.

- Governing body means the committee of the Board of Trustees to which Trustees have delegated appropriate powers and functions relating to the governance of the school.
- School IT Lead is the individual in their school to whom the Principal has delegated responsibility for IT related matters in school.

In this procedure references to the Athena Learning Trust will be read as including the Athena Learning Trust shared service and all schools in the Athena Learning Trust.

References in this Procedure to a school in the Trust should also be read as the Trust Shared Service for services, functions and members of staff of the Trust that are not contained within a school budget and/or are not the responsibility of a Principal and/or Governing Body. With respect to the Trust Shared Service, references in this Procedure to the responsibilities of the Principal and Governing Body should be read as the Athena Learning Trust CEO and the Trust Shared Services Committee respectively.

1.4. Responsibilities

It is the responsibility of the Principal of each school, and Athena Learning Trust CEO for the Trust Shared Service, to ensure that their school/service and its staff adhere to this Athena Learning Trust Cyber Security Procedure; in implementing this Procedure the Principal and Trust staff must take account of any advice given to them by the Athena Learning Trust Head of IT, Athena Learning Trust CEO and/or Board of Trustees.

Each Principal will appoint an individual as School IT Lead to be the point of contact for staff, students and parents, and to liaise with the Athena Learning Trust Head of IT for matters relating to IT and to this procedure within their school. The Principal must provide the name and contact details of the School Lead to the Athena Learning Trust Head of IT.

1.5. Associated policies and procedures

This Procedure is a constituent part of the Athena Learning Trust Communications Policy.

PART B

1. Purpose and scope

1.1 The purpose of this Procedure is to establish systems and controls to protect the Athena Learning Trust and its schools from cyber criminals and associated cyber security risks, and to ensure that appropriate action is taken should the Trust or any of its schools fall victim to cyber-crime.

1.2 This Cyber Security Procedure applies to all IT systems used by the Trust and its schools including:

- Computers (Desktops, Laptops, Smartphones, Tablets, Servers).
- Telephony Hardware.
- Internet Routers and Firewalls.
- Wired and Wireless Networking Hardware.
- All software and operating systems used on trust and school devices.
- 3rd party systems (e.g. HR Portal, IT Helpdesk, Premises Management System).
- Cloud based systems (e.g. Google Workspace, Office 365).

1.3 It is important, given the serious consequences of a cyber-attack, to be careful not to be the victim and to follow this procedure.

2. Introduction

2.1 **What is Cyber Security?** - Cyber security is how individuals and organisations reduce the risk of a Cyber attack. Its core function is to protect the devices that an organisation uses (smartphones, laptops, tablets, as well as local onsite and cloud based server infrastructure), from theft or damage and to prevent unauthorised access to the vast amounts of personal information that are stored on these devices, and on local servers and in the Cloud.

2.2 **What is a Cyber Attack?** - Cyber attacks are a risk for the for the Athena Learning Trust and all of its schools. A cyber attack attempts to damage, disrupt or gain unauthorised access to computer systems, networks, devices and the data they contain. It can take shape in a variety of different forms, e.g. hacking, phishing emails, malware, viruses or ransomware attacks.

2.3 **Impact of a Cyber Attack** – Cyber attacks can have a devastating impact on

organisations, with victims requiring a significant amount of recovery time to reinstate critical services. These events can also be high profile in nature, with wide public and media interest. In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing. A cyber-attack can trigger a breach investigation by the Information Commissioner's Office (ICO).

2.4 **Who is responsible for Cyber Security?** – It is the responsibility of **all** members of staff, Trustees and governors within the Trust and **all** need to contribute towards cyber security. The Principal retains accountability for cyber security within the school and may delegate responsibility to the School IT Lead for IT systems management. The School IT Lead will follow the advice of the Athena Learning Trust Head of IT. The Athena Learning Trust Head of IT retains accountability for Cyber Security within the Trust Shared Service and responsibility for its IT Systems Management will be the responsibility of the Athena Learning Trust Head of IT.

2.5 **Disciplinary action** – A member of staff, Trustee or Governor of the Trust may be subject to disciplinary action should they breach this procedure.

2.6 Any member of staff, Trustee or Governor that is aware of or suspects a cyber attack or has a concern relating to a cyber security should immediately notify the Athena Learning Trust Head of IT or the appropriate School IT Lead, who will notify the Athena Learning Trust Head of IT and the Principal.

3. Prevention

3.1 The School IT Lead must put in place systems and controls to mitigate the risk of the school falling victim to a cyber-attack, taking the advice of the Athena Learning Trust Head of IT. These include technology based solutions as well as controls and instructions to all staff. These will include

i. Firewalls (Correctly configured – as per manufacturers guidance).
ii. Anti-virus and malware software.
iii. Anti-Spam filtering for email.
iv. Automatic updates for systems and applications.
v. Internet Filtering.
vi. Secure backups of all data both onsite and hosted. minimum 3 copies including one that is offsite or offline.

vii. Use of strong passwords.
viii. Factor Authentication.
ix. Encryption (where there is a risk of devices or data falling into the wrong hands).
x. Processes for deleting or disabling unused redundant user accounts.

4. Controls and guidance for staff

4.1 All staff will be provided with training and refresher training as appropriate including, 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 data is shared.

4.2 Every member of staff, Trustees and Governors must:

i. Choose a password with a minimum of 8 characters, including upper and lower case, numbers and punctuation characters.
ii. Keep passwords a secret unless it is the Principal and their PA or the CEO and their EA
iii. Never reuse a password (or have the same password for 2 different logins).
iv. Never allow any other person to access the school / Trust systems using their login details.
v. Not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that has been installed on their computer, phone or the school IT systems.
vi. Report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to the School IT Lead, as soon as practicable from the time of the discovery or occurrence.
vii. Not install software on any school or Trust IT system without authorisation of the School IT Lead.
viii. Avoid clicking on links to unknown websites, or accessing inappropriate content using school / Trust IT systems.

4.3 Every member of staff, Trustee and Governor must ensure that they do not misuse any of the Trust's IT systems. The Trust considers the following actions to be a misuse of its IT systems or resources:

1.1.1 Any malicious or illegal action carried out against the school / Trust or using

the school / Trust systems.

1.1.2 Accessing inappropriate, adult or illegal content within school / Trust premises or using school / Trust equipment.

1.1.3 Excessive personal use of school / Trust IT systems during working hours.

1.1.4 Removing data or equipment from school / Trust premises or systems without permission, or in circumstances prohibited by this procedure.

1.1.5 Using school / Trust equipment in a way prohibited by this procedure.

1.1.6 Failing to report a mistake or cyber security breach.

5. Cyber-attack incident management plan

5.1 The Principal must ensure that their school has an incident management plan that encompasses the stages below, and that the plan is implemented in the event of cyber attack or suspected cyber attack occurring:

Stage 1 - Containment and recovery – Immediately a cyber attack is discovered or suspected it must be reported to Athena Learning Trust Head of IT. The incident must be investigated utilising appropriate staff to mitigate damage and recover any data lost where possible.

Stage 2 -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.

Stage 3 - Athena Learning Trust *Head of IT – to make the decision if this is reported to the ICO* to consider if the cyber-attack needs to be reported to regulators (for example the ICO / DfE) and/or colleagues/parents as appropriate.

Stage 4 - Evaluation and response to consider any improvements to data security and evaluate future threats to security.

5.2 Where a cyber security incident may involve a personal data breach, the Principal will ensure the Data Breach Procedure is also followed.