KING EDWARD VI
ACADEMY TRUST
BIRMINGHAM

INFORMATION SECURITY POLICY

Responsible Board	Academy Trust Board
Policy Officer	IT Officer
Date Adopted	October 2018
Review Date	October 2020

KING EDWARD VI ACADEMY TRUST BIRMINGHAM INFORMATION SECURITY POLICY

1. Introduction

The Academy Trust is responsible for the security and integrity of all data it holds. It must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the Academy Trust's assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security, including but not limited to:

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
    - loss of confidentiality of information
    - compromise of integrity of information
    - denial of service
    - unauthorised access to systems
    - misuse of systems or information
    - theft and damage to systems
    - virus attacks
    - intrusion by humans

- Other incidents include:
    - Exposure of Uncollected print-outs
    - Misplaced or missing media
    - Inadvertently relaying passwords
    - Loss of mobile phones and portable devices

Ensuring efficient reporting and management of security incidents will help reduce and, in many cases, prevent incidents occurring.

More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

2. Purpose

The management of IT security incidents described in this policy requires the Academy Trust to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed; sometimes over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide guidance

3. Scope

This policy applies to:

- Academy Trust employees, volunteers and Governors/Trustees (the 'Users').
- All Academy Trust systems (including software) dealing with the storing, retrieval and accessing of data.

4. Policy Statement

The Academy Trust has a clear incident reporting mechanism in place (see section 8 below) which details the procedures for the identifying, reporting and recording of IT security incidents. By continually updating and informing users of the importance of the identification, reporting and action required to address incidents, the Academy Trust can continue to be pro-active in addressing these incidents as and when they occur.

All users are required to report all incidents – including potential or suspected incidents, as soon as possible via the Academy Trust's Incident Reporting procedures.

The types of Incidents which this policy addresses includes but is not limited to:

Computers left unlocked when unattended

Users of Academy Trust IT systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All users need to ensure they lock their computers appropriately. Discovery of an unlocked computer which is unattended must be reported via the Academy Trust's Incident Reporting procedures.

Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others regardless of trust. If an individual needs access to data or a system, they must use the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed, whether intentionally, inadvertently or accidentally, the IT Support Technician must be notified. Under no circumstances should an employee allow another employee to use their user account details even under supervision.

Virus warnings / alerts

All Desktop and laptop computers in use across the Academy Trust have Antivirus software. The interaction between the computer and antivirus software will usually go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected that could cause loss, theft or damage to Academy Trust data. The warning message may indicate that the antivirus software may not be able to rectify the problem and must therefore be reported by the user to the IT Support Technician as soon as possible.

Media loss

Use of portable media such as CD/DVD/USB Flash sticks/HD drives for storing data require the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device (including portable media) who has misplaced or suspects damage or theft whether intentional or accidental must report it immediately through the Academy Trust's Incident Reporting procedures.

Data loss / disclosure

The potential for data loss applies not only to portable media but also to any data that is:

- Transmitted over a network and reaching an unintended, unauthorised recipient (such as the use of email to send sensitive data);
- Intercepted over the internet through non-secure channels;
- Posted on the internet whether accidental or intentional;
- Published on the Academy Trust's website and identified as inaccurate or inappropriate;

- Conversational: information disclosed during conversation;
- Press or media: unauthorised disclosure by employees or an ill-advised representative to the press or media;
- No longer located and is unaccounted for on an IT system;
- Unlocked and uncollected (e.g. print-outs from Multi-Function Devices (MFDs));
- Paper copies of data and information that can no longer be located; and
- Hard copies of information and data accessible from desks and unattended areas.

All users must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Academy Trust data at all times.

Any loss of data and/or disclosure, whether intentional or accidental, must be reported immediately using the Academy Trust's Incident Reporting procedures

Personal information abuse
All personal identifiable information i.e. information which can identify an individual such as home address, bank account details etc. must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such personal identifiable information must be reported through the Academy Trust's Incident Reporting procedures.

Physical Security
Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room e.g. a combination key lock mechanism. Lower/floor level windows that could provide access to the room/office must also be securely locked particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data; concerns about any rooms/office which should be securely locked or access restricted must be reported to the IT Desktop Support Technician.

Logical Security / Access Controls
Controlling, managing and restricting access to the Academy Trust and Academies Networks, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorised employees can gain access to information which is processed and maintained electronically.

Missing correspondence
Data or information which has been sent either electronically or physically that cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc. must be reported through the Academy Trust's Incident Reporting procedures.

Found correspondence / media
Data stored on any storage media or physically printed information that has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through the Academy Trust's Incident Reporting procedures.

Loss or theft of IT / information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc. or which is known/suspected to have been stolen needs to be reported immediately through the Academy Trust's Incident Reporting procedures.

5. Responsibilities

It is the responsibility of all users who undertake work for the Academy Trust, on or off the premises, to be proactive in the reporting of security incidents. The Academy Trust's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Academy Trust data and information.

It is also a responsibility of all individuals and handlers of Academy Trust data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

6. Compliance with legal and contractual obligations

The Data Protection Act 2018 and the General Data Protection Regulation 2016 requires that personal data be kept secure against unauthorised access or disclosure.

The Computer Misuse Act (1990) covers unauthorised access to computer systems.

7. Breaches of Policy

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Academy Trust's assets, including IT equipment and information, or conduct which is in breach of the Academy Trust's Computer Security Incident procedures and policies.

All users have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Academy Trust's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Academy Trust.

In the case of third-party vendors, volunteers or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Academy Trust IT systems or network results from the non-compliance, the Academy Trust will consider legal action against the third party. The Academy Trust will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee, infringements will be investigated under the disciplinary procedure and progressed as appropriate.

8. Computer Security Incident Reporting Procedure

The IT Support Technician will continually highlight the importance of incident reporting and will further encourage the methods by which security breach incidents can be reported. Where computer access to the Academy Trust's network or e-mail is not available, breaches can be reported via a telephone call to the IT Desktop Support Technician. Breaches can involve not only Information Technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern, or which may contravene the policies.

Any breach of the Incident Management Policy must be reported as soon as possible via the reporting procedure.

There are various ways in which computer security incident breaches can be reported.

We recommend computer security incidents/breaches to be recorded via:

- A phone call to the IT Support Technician
- E-mailing the IT Desktop Support Technician
- Visiting the IT Desktop Support Technician

The following information should be included:

- Incident Date/Time
- Computer
- Department
- Location
- Contact details: phone, email address etc.
- Type of incident
- Description: more detailed information about the incident

When an incident is reported the IT Support Technician and the Data Protection Officer will then determine if the incident needs to be escalated to SLT to investigate as soon as possible.

All parties dealing with computer security incidents shall undertake to:

- analyse and establish the cause of the incident and take any necessary steps to prevent recurrence;
- report to all affected parties and maintain communication and confidentiality throughout investigation of the incident;
- identify problems caused as a result of the incident and prevent or reduce further impact;
- contact third parties to resolve errors/faults in software and to liaise with the relevant IT Department and departmental personnel to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Academy Trust systems and services;
- ensure all system logs and records are securely maintained and available to authorised personnel when required;
- ensure only authorised personnel have access to systems and data;
- ensure all documentation and notes are accurately maintained and recorded in the Incident Management log and made available to relevant authorised personnel; and
- ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness

Where appropriate, incidents will be presented to the Data Protection Officer and/or SLT. All incidents reported shall record all the details of the incident in the Incident Management Log including any action and/or resolution, links or connections to other known incidents. Incidents which were initially resolved but have recurred will be reopened or a new record referencing the previous incident/s will be created.

Periodic analysis of incidents should be conducted to monitor the types, numbers, frequency and severity of incidents to help inform, correct and prevent incidents recurring.

During the course of incident investigations, hardware, logs and records may be analysed by the IT Support Technician. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential that confidentiality is maintained at all times during the course of these investigations.

The IT Support Technician is initially responsible for handling computer security incidents and will decide whether an incident should be escalated and dealt with by a member of the SLT or the Data Protection Officer.

This document forms part of the Academy Trust's ICT Policies and must be fully complied with.