CYBER SECURITY POLICY

Policy Approval	
JUDICIUM & EDUCATION We take care of it	February 2023
Approved by Trust Board:	Meeting Date: 08/02/23 Minute No: 11
Review Date:	September 2024

Introduction

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

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

The Network Manager is responsible for cyber security within the Trust.

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, Home Working Policy, Bring Your Own Device Policy and Electronic Information and Communications Policy.

Purpose and Scope

The purpose of this document is to establish systems and controls to protect the Trust from cyber criminals and associated cyber security risks, as well as to set out an action plan should the Trust 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 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;
- 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 Trust 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 Network Manager can provide further details of other aspects of the Trust risk assessment process upon request.

The Trust 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.

All schools within the Trust are registered with the PoliceCyberAlarm and the National Cyber Security Centre.

Technology Solutions

The Trust 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 user accounts;

(ix) deleting or disabling unused/unnecessary software;

(x) using strong passwords; and

(xi) disabling auto-run features.

Controls and Guidance for Staff

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

- 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 Trust or any third parties with whom we share data. This includes completion of the National Cyber Security Centre's Cyber Security Training.

- All staff must:

- Choose strong passwords the Trust's IT team advises that a strong password meets the following criteria:

  Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
  Be at least 7 characters in length.
  Contain characters from three of the following four categories:
  English uppercase characters (A through Z).
  English lowercase characters (a through z).
  Base 10 digits (0 through 9).
  Non-alphabetic characters (for example, !, $, #, %);

- keep passwords secret;

- never reuse a password;

- never allow any other person to access the Trust's systems using your login details;

- 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 Trust IT systems;

- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the Network 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 the Trust owns. Staff may only connect personal devices to the visitor Wi-Fi provided;

- not install software onto your Trust computer or phone. All software requests should be made to the Network Manager; and

- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using Trust equipment and/or networks.

- The Trust considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the Trust or using the Trust's systems;

- accessing inappropriate, adult or illegal content within Trust premises or using Trust equipment;

- excessive personal use of Trust's IT systems during working hours;

- removing data or equipment from Trust premises or systems without permission, or in circumstances prohibited by this policy;

- using Trust equipment in a way prohibited by this policy;

- circumventing technical cyber security measures implemented by the Trust's IT team; and

- failing to report a mistake or cyber security breach.

Cyber-Crime Incident Management Plan

The incident management plan 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 Trust will invoke their Data Breach Policy rather than follow out the process above.