Westcountry Schools Trust (WeST)

Cyber Security Procedure

Mission Statement

WeST holds a deep seated belief in education and lifelong learning. Effective collaboration, mutual support and professional challenge will underpin our quest to ensure that all of the children and adults we serve are given every opportunity to fulfil their potential and succeed in life.

Person(s) responsible for updating the policy:	WeST IT Operations Lead
Date Approved:	Trust Board 14 Dec 2022
Date of next review:	October 2023
Status: Statutory / Non-statutory	Non-Statutory
Published on	WeST Website

WeST Core Values
WeST holds four core values which underpin the engagement, motivation and retention of employees, no matter what their role in the organisation.

· Collaboration

Creating a shared vision and working effectively across boundaries in an equitable and inclusive way to skilfully influence and engage others. Building and securing value from relationships, developing self and others to achieve positive outcomes.

· Aspiration

Having high expectations, modelling the delivery of high-quality outcomes. Showing passion, persistence and resilience in seeking creative solutions to strive for continuous improvement and excellence.

· Integrity

Acting always with the interests of children and young people at our heart, and with a consistent and uncompromising adherence to strong moral and ethical principles. Communicating with transparency and respect, creating a working environment based on trust and honesty.

· Compassion

Recognising need in others and acting with positive intention to promote well-being and improve outcomes.

Providing Accessible Formats

If you require this policy in an accessible format, please contact admin@weststst.org.uk

Westcountry Schools Trust Cyber Security Procedure

Contents

PART A

1.1. Application

This Westcountry Schools Trust (WeST) Cyber Security Procedure applies to the Westcountry Schools Trust as a whole and to all the schools in the Trust and the Trust's Central Services.

All WeST employees, trustees and those in governance must abide by this WeST 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, a school's Headteacher and their employees must take account of any advice or instruction given to them by WeST's Information Technology (IT) Operations Lead, or its CFO, CEO or Board of Trustees.

If there is any question or doubt about the interpretation or implementation of this Procedure, the WeST IT Operations Lead should be consulted.

1.2. Approval and review

Maintenance of this Procedure is the responsibility of the WeST IT Operations Lead via the IT Sub-Committee and Audit and Risk Committee. It should be reviewed every two years.

This procedure was approved by the Board of Trustees on: 14 December 2022.

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

1.3. Terminology

The Trust means the Westcountry Schools Trust (WeST).

- School means a school within the Westcountry Schools Trust.
- Headteacher means the Headteacher or Principal of the school.
- CFO means the Chief Financial Officer of WeST;
- CEO means the Chief Executive Officer of WeST;
- DPO means the Data Protection Officer of WeST;
- Those in governance and Trustees includes those in the WeST local tier of governance, trustees, and non-trustee members of Trust Committees;

- Local tier of governance means the local bodies to which trustees have delegated appropriate functions relating to governance in accordance with the Scheme of Delegation;
- School IT Lead is the individual in each WeST school to whom the Headteacher has delegated responsibility for IT related matters in school.

In this procedure references to the Westcountry Schools Trust will be read as including the Westcountry Schools Trust central service, all schools in the Westcountry Schools Trust and The Learning Institute (TLI).

References in this Procedure to a school in the Trust should also be read as the Trust Central Service and TLI 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 Headteacher and/or governance structure. With respect to the Trust Central Service and TLI , references in this Procedure to the responsibilities of the Headteacher and local tier of governance should be read as the WeST CEO and Trust Board.

1.4. Responsibilities

It is the responsibility of the Headteacher of each school, and WeST CEO for the Trust Central Service and TLI, to ensure that their school/service and its staff adhere to this WeST Cyber Security Procedure; in implementing this Procedure the Headteacher and Trust staff must take account of any advice given to them by the WeST's IT Operations Lead, CFO, CEO and/or Board of Trustees.

Each Headteacher will appointing an individual as School IT Lead to be the point of contact for staff, students and parents, and to liaise with the WeST IT Operations Lead for matters relating to IT and to this procedure within their school. The Headteacher must provide the name and contact details of the School Lead to the WeST IT Operations Lead.

1.5. Associated policies and procedures

This Procedure is an associated part of the WeST Anti Fraud and Corruption Policy

PART B

1. Purpose and scope

1.1 The purpose of this Procedure is to establish systems and controls to protect WeST 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 WeST and/or school devices;
- 3rd party systems (e.g. HR Portal, IT Helpdesk, PS Financials System, and SIMS); and
- Cloud based systems (e.g. IMP, CPOMS, and 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 WeST 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 cyberattack 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 those in governance within the Trust and all need to contribute towards cyber security. The Headteacher 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 WeST IT Operations Lead. The CEO retains accountability for Cyber Security within the Trust Central Service and TLI, whilst responsibility for its IT Systems Management will be the responsibility of the WeST IT Operations Lead .

2.5 Disciplinary action – A member of staff, trustee or member of the local governance tier of the Trust may be subject to disciplinary action when they breach this procedure.

2.6 Any member of staff, trustee or member of the local governance tier that is aware of or suspects a cyber attack or has a concern relating to a cyber security should immediately notify the WeST IT Operations Lead or the appropriate School IT Lead, who will notify the WeST IT Operations Lead and the Headteacher.

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 WeST IT Operations Lead. These include technology based solutions as well as controls and instructions to all staff. These will include Trust approved:

- Firewalls (correctly configured – as per manufacturers guidance);
- Anti-virus and malware software;
- Anti-Spam filtering for email;
- Automatic updates for systems and applications;

- Internet Filtering;
- Secure backups of all data both onsite and hosted - minimum 2 copies including one that is offsite or offline;
- Use of strong passwords;
- Two Factor Authentication;
- Encryption (where there is a risk of devices or data falling into the wrong hands) and
- 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 Central.

4.2 Every member of staff, trustees and member of the local governance tier must:

- Choose a password with a minimum of 8 characters, including upper and lower case, numbers and punctuation characters;
- Keep passwords a secret;
- Never reuse a password (or have the same password for 2 different logins);
- Never allow any other person to access the school / Trust systems using their login details;
- 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;
- Report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to the School IT Lead and DPO as soon as practicable from the time of the discovery or occurrence;
- Not install software on any school or Trust IT system without authorisation of the School IT Lead; and
- Avoid clicking on links to unknown websites, or accessing inappropriate content using school / Trust IT systems.

4.3 Every member of staff, trustee and member of the local governance tier 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:

- Any malicious or illegal action carried out against the school / Trust or using the school / Trust systems;
- Accessing inappropriate, adult or illegal content within school / Trust premises or using school / Trust equipment;
- Excessive personal use of school / Trust IT systems during working hours;
- Removing data or equipment from school / Trust premises or systems without permission, or in circumstances prohibited by this procedure;
- Using school / Trust equipment in a way prohibited by this procedure; and
- Failing to report a mistake or cyber security breach.

5. Cyber-attack incident management plan

5.1 The Headteacher 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 WeST IT Operations Lead. 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 - WeST *IT Operations Lead in conjunction with WeST's DPO and/or CFO – 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 reporting back to the Trust's IT Sub-Committee

5.2 Where a cyber security incident may involve a personal data breach, the Headteacher will ensure the Data Breach Procedure is also followed including without limitation notifying immediately WeST's DPO.

Adoption of the Procedure
This procedure has been adopted by the Trustees of the Westcountry Schools Trust

Signed
Iain Grafton

Chair of Trust
Trust Board meeting Date 14 Dec 2022