Units 13 & 14, Malt Store Annex
The Cut, 8 New Cut, Halesworth
Suffolk IP19 8BY

enquiries@suffolkartlink.org.uk
www.suffolkartlink.org.uk
01986 873 955

Suffolk.Artlink
@Suffolk_Artlink

Cyber Safeguarding: Security Incident Management Policy and Procedure

1. Purpose

The purpose of this policy and procedure is to set out how Suffolk Artlink will prevent, identify, manage and respond to cyber security incidents and cybercrime that could cause harm to the charity or to people connected with it.

We are committed to safeguarding our staff, volunteers, beneficiaries and trustees from harm arising from cyber-attacks, data loss, misuse of information, or disruption to services.

Cyber incidents may be opportunistic or targeted, originate from outside or within Suffolk Artlink, or result from physical events such as fire, flood, theft or equipment failure.

This policy and procedure aims to protect the confidentiality, integrity and availability of critical organisational information, including but not limited to:

- Beneficiary records
- Staff and volunteer personal data
- Governance and operational documents
- Financial, banking and payment information

Registered charity number 1110898
Company number 05354844

2. Scope

This policy applies to everyone working/ volunteering on behalf of Suffolk Artlink, including the board of trustees.

3. Policy

We are committed to preventing, identifying and managing cyber security incidents that could cause harm to individuals or disrupt organisational operations. We will take proportionate steps to protect sensitive information, maintain secure and recoverable data systems, and ensure continuity of services following cyber or physical incidents. Cyber safeguarding is a shared responsibility, overseen by trustees and supported by informed staff and volunteers.

All staff, volunteers and trustees will be supported to understand cyber risks and their role in protecting both themselves and Suffolk Artlink. This includes awareness of common threats such as phishing, malware and data breaches, and knowing how to report concerns or incidents quickly.

Trustees have overall responsibility for cyber safeguarding and will set clear expectations for preventing and responding to cyber incidents, including:

- The actions trustees, staff and volunteers must take when a suspected cyber incident is identified
- The cyber security and data protection training required to maintain appropriate knowledge, awareness and good practice

Through this policy and procedures Suffolk Artlink aims to strengthen its cyber resilience, protect those it works with, and ensure the continuity, safety and integrity of its services. We take a multifaceted approach of Prevent. Respond. Report.

4 Procedures: Security Incident Plan

To reduce risk and improve resilience, Suffolk Artlink will maintain regular and secure backups of important data. Backup frequency will be determined by risk and potential impact, with agreed schedules followed and regularly reviewed. Backups will be tested to ensure data can be accessed and restored promptly, enabling Suffolk Artlink to continue operating and recover quickly following a cyber or physical incident.

Prevent

- We will identify our essential data for backup. This is the information we could not operate without access to. It includes documents, emails, contacts, legal information, calendars, financial records, CRM database and beneficiary details
- The backup will be kept separate from the main network, on a separate drive or a separate computer/ the cloud. USB, access to data backups are restricted so that they:

- are not accessible by all staff or volunteers
    - are not permanently connected (either physically or over a local network) to the device holding the original copy
- We will identify and install suitable firewall/ antivirus software to all laptops, mobile phones and any other devices.

• IT equipment software will be kept up to date.

• We will not use non sanitised previously owned IT equipment including unknown USB devices.

• Laptops and computers will have password protection enabled.

• Mobile phones will have screenlocks on and notifications do not show on lock screens.

• Lost or stolen devices can be tracked, locked or wiped by using appropriate mobile device management software.

• Only apps from manufacturer approved stores (Google Play, Apple App Store) will be downloaded and we will not download third party apps from unknown vendors/sources

• We will not connect mobile devices to unknown 'hotspots' or public WiFi networks, for example in coffee shops or public transport as there is no easy way to find out who controls the hotspot, or to be assured it's secure.

• We will follow our IT and social media policies and procedures.

• Trustee will be aware of Cyber Security Toolkit for Boards, from the National Cyber Security Centre https://www.ncsc.gov.uk/collection/board-toolkit/toolkits-toolbox/downloads

• Cyber incidents are included in our Business Continuity Plans.

Respond

• Any actual or suspected cyber-attack will be reported to the General Manager immediately. Other staff to be made aware depending on the severity including the Trustee responsible for cyber security, who will decide the next step. Seek professional support from Suffolk Artlink's designated provider, Atec Solutions, if required:
John Feeny-Howells, jfh@atec.co.uk, 07818 402362
Peter Woods, peter@atec.co.uk, 01728 861777

• The nature of the incident will be identified e.g.

◦ Malicious code: Malware infection on the network, including ransomware

◦ Denial of service: Typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems

◦ Phishing: Emails attempting to convince someone to trust a link/attachment.

◦ Unauthorised access: Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account.

◦ Insider: Malicious or accidental action by an employee causing a security incident.

◦ Data breach: Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).

◦ Targeted attack: An attack specifically targeted at the business - usually by a sophisticated attacker (often encompassing several of the above categories).

From https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes#escalate

• The severity of the incident will be determined and we will respond to any actual or suspected cyber attack quickly to help reduce the harm to Suffolk Artlink and beneficiaries.

• Legal and or insurance advice will be sought if necessary

• We will keep a record of what happened, and when

• If we are currently experiencing an incident, we can contact the NCSC.

Report

Step 1 If it is assessed that there has been a cyber incident, it must be reported to Action Fraud by calling 0300 123 2040, or by visiting the Action Fraud website.

Step 2 If it is assessed that a cyber incident constitutes a 'serious incident' it must be reported to the Charity Commission. A serious incident is defined by the Charity commission as "an adverse event, whether actual or alleged, which results in or risks significant:

• harm to your charity's beneficiaries, staff, volunteers or others who come into contact with your charity through its work

• loss of your charity's money or assets

• damage to your charity's property

• harm to your charity's work or reputation

Step 3 If it is assessed that a cyber incident has occurred it will agreed which, if any, other parties need to be informed.

Step 4 If Suffolk Artlink suffers a loss of 'personal data' the Information Commissioner's Office must be informed.

Step 6 An appropriate post incident review will take place where lessons from the incident, response and reporting will be identified and learned from.

• What happened, what could have prevented it or allowed earlier identification? Was there any information that would have helped our response but we couldn't find or access?

• Was the response effective? What went well and what could be improved upon? Were the right people involved and able to make the necessary decisions?

5.Monitoring and Review

The Board and Director will review this policy triennially or after an incident highlights a gap.

The Board of Trustees will review this policy triennially.

28th July 2025	AW	Company Secretary on behalf of the Board of trustees
