Cybersecurity Policy

Juliet Diener
Founder & Chief Executive Officer
juliet@icandance.org.uk

Cybersecurity Policy

Document created by:	Created On:
Juliet Diener	June 2025
Reviewed Last	N/A

To be reviewed by:	Review date:
CEO	June 2028

Signed by : Juliet Diener

Date : June 2025

1) The Purpose of this Policy

This cybersecurity policy aims to protect the personal data of children and young people (CYP), staff, and volunteers at icandance by ensuring secure digital practices and protecting against data breaches, unauthorized access, and cyber threats.

2) Scope

This policy applies to:

- All team members, volunteers, contractors, external partners, and trustees who access icandance's digital systems.
- All digital devices (computers, tablets, mobile phones) and platforms (email, cloud storage, websites) are used in the organisation.

3) icandance's Responsibilities

At icandance, all team members, volunteers, contractors, and trustees share a collective responsibility to uphold cybersecurity and protect personal and sensitive data. This includes:

- **Safeguarding data**: Ensuring all personal, sensitive, and confidential data is collected, stored, and shared securely in accordance with this policy and applicable laws.

- **Using technology responsibly**: Only using authorised devices, systems, and platforms for charity-related communication and data handling.

- **Maintaining vigilance**: Being alert to cybersecurity threats (e.g. phishing emails, suspicious links, malware) and reporting incidents promptly to the designated lead.

- **Following access controls**: Respecting permissions, not accessing information beyond one's role, and never sharing login credentials.

- **Engaging in training**: Completing required cybersecurity and data protection training and refreshers to stay informed about best practices.

- **Contributing to a safe culture**: Supporting a culture of security and responsibility by encouraging team-wide compliance and raising awareness of new risks or breaches.

Senior leadership holds overall accountability for implementing and reviewing this policy and ensuring adequate resources and training are in place to protect the organisation's digital infrastructure and data.

4) Definitions

Roles

- **Senior Leadership** – Those responsible for strategic and operational management of the charity (e.g. CEO and team leads).
- **Team Member** – All paid staff, volunteers, interns, and contracted personnel working with or on behalf of the charity.

Data Protection & Access

- **Personal Data** – Any information relating to an identified or identifiable individual (e.g., name, email, address).
- **Sensitive Personal Data** – Information such as health details, ethnicity, religious beliefs, or data concerning a child, which requires higher protection. They can access by senior leadership unless with approval
- **General Information** – Publicly available or non-sensitive data such as session types, event dates, or venue names.
- **Photographic Data** – photos of individuals at icandance, including children, young people and team members.
- **Data Breach** – A breach of security leading to accidental or unlawful destruction, loss, alteration, disclosure of, or access to, personal data.
- **Access Control** – Systems and protocols in place to ensure only authorised individuals can access specific data or resources.

Communication & Sharing

- **Secure Communication** – The use of encrypted and approved platforms (e.g., Outlook, Microsoft Teams, Google Workspace) for sharing sensitive or personal information.
- **Disappearing Messages** – A messaging feature (e.g., WhatsApp) that auto-deletes messages after a set period to reduce the risk of data retention.

Cybersecurity

- **Two-Factor Authentication (2FA)** – An additional login security measure requiring two forms of verification (e.g., password + code sent to phone).
- **Encryption** – A method of converting data into a coded format to prevent unauthorised access.
- **Phishing** – A type of online scam where attackers impersonate legitimate entities to trick users into revealing sensitive information.

5) Legal Framework

This policy is guided by the following UK legal and regulatory frameworks to ensure the protection of personal data and secure digital practices:

- **Data Protection Act 2018 (DPA 2018):** Aligns UK data protection law with the EU General Data Protection Regulation (GDPR) and governs how personal data must be collected, stored, and used.
- **UK General Data Protection Regulation (UK GDPR):** Sets out principles, rights, and obligations for handling personal data, including consent, data minimisation, and security measures.
- **Computer Misuse Act 1990:** Prohibits unauthorised access to computer systems and provides a legal framework for cybercrime prevention.
- **Children's Code (Age-Appropriate Design Code):** Applies to online services likely to be accessed by children, requiring extra safeguards to protect children's data and privacy.

icandance is registered with the Information Commissioner's Office (ICO) and maintains its registration through annual renewal, demonstrating our commitment to data protection compliance.

6) Data Protection

icandance is committed to protecting the personal data of children, young people, staff, volunteers, and families in line with UK data protection legislation. The following principles guide our handling of personal data:

- **Purpose Limitation:** We only collect **personal data** (e.g. names, contact details, health and safeguarding information) that is **strictly necessary** to carry out the charity's legitimate activities. Data will not be collected or retained for purposes unrelated to our offer.
- **Data Minimisation & Accuracy:** We aim to **minimise the amount of data collected** and ensure that all information held is accurate, up to date, and relevant. Regular audits will be conducted to review stored data and ensure its necessity and accuracy.
- **Secure Storage:** All personal data must be stored in **encrypted** or **password-protected** systems (e.g. secure cloud platforms). Data must **never** be stored on unencrypted local devices. icandance does not keep any physical files.

- **Controlled Sharing and Consent:** Personal data must **never be shared externally or internally** without appropriate written consent from senior leadership, unless sharing is **required by law** (e.g. safeguarding concerns). Staff and volunteers must follow designated procedures when requesting or granting access to data.

- **Retention and Deletion:** Data will be retained only for as long as necessary to fulfil its intended purpose. For example, dancer records are deleted 7 years after a participant has left icandance unless there is a legal or safeguarding reason to retain them longer.

- **Data Subject Rights:** Individuals have the right to access their data, request corrections, or request information to be deleted. Requests must be actioned within one month.

7) Secure Access Control

To maintain the integrity and security of sensitive data, icandance enforces strict access control protocols across all digital systems:

- **Strong Password Requirements:** All staff, volunteers, and contractors must use strong passwords (a minimum of 10 characters, and include a mix of uppercase and lowercase letters, numbers, and symbols). Passwords must never be shared or reused across systems. Organisational passwords are securely stored in encrypted password management tool (OneDrive).

- **Multi-Factor Authentication (MFA):** Wherever supported, two-factor or multi-factor authentication (2FA/MFA) is used on accounts, especially those involving access to sensitive personal data or financial information.

- **Regular Password Updates:** All passwords should be updated at least every 6 months. Any suspected compromise must result in an immediate password change and be reported to the operations coordinator.

- **Role-Based Access Control (RBAC):** Access to data and systems will be restricted based on role. Users will only be granted access to the minimum necessary information required to perform their duties. This prevents unauthorised access and limits the risk of data exposure.

- **Account Deactivation & Exit Procedure:** Accounts for team members who leave the organisation must be promptly deactivated. Devices and login credentials must be returned or disabled within 24 hours of exit.

- **Audit and Review:** Access permissions will be reviewed quarterly, and immediately upon role changes or terminations. The CEO will maintain an access log for all sensitive systems.

8) Safe Communication

To ensure the protection of sensitive information, all communication, whether internal or external, must adhere to secure, privacy-conscious practices:

- **Approved Communication Channels:** Team members must use secure, organisation-approved platforms such as Outlook, Gmail with organisational accounts, Microsoft Teams, or other encrypted email services for transmitting sensitive or personal data. These platforms support encryption and user access control to safeguard information.

- **Prohibited Use of Unsecured Channels:** Do not share sensitive or personal information (e.g., full names, addresses, medical details) via unsecured platforms such as personal WhatsApp, SMS, Facebook Messenger, or non-organisation email addresses. If messaging apps are used in exceptional cases (e.g., WhatsApp), they must use disappearing messages, and only with prior approval from senior leadership. Photos should only be shared via Teams or an icandance email unless with consent from senior leadership team.

- **Use of BCC for Group Emails:** When emailing groups of children, parents, or external contacts, always use the Blind Carbon Copy (BCC) field to prevent recipients from seeing each other's email addresses. This protects privacy and ensures GDPR compliance.

- **Sharing Sensitive Documents:** Sensitive documents should only be shared via password-protected cloud storage links (e.g., Google Drive, OneDrive) with access permissions set to "view only" or time-limited access. Do not attach sensitive documents directly to emails unless they are encrypted or only for internal purposes. No identifiable images of children should be shared via messaging apps unless encrypted and consented.

- **Internal Communication Best Practices:** Refrain from discussing confidential matters in general team chats or channels. Designate specific secure spaces (e.g., private Teams channels, private Zoom meetings, or shared drives with restricted access) for operational discussions involving personal data.

- **Third-party Communication:** When sharing information with external organisations (e.g., schools, therapists), confirm the identity of recipients and ensure that communication is secure and justified under data protection laws.

- **Awareness and Caution:** All staff and volunteers must be trained to recognise phishing attempts, spoofed email addresses, and suspicious links. Any unexpected requests for personal data or unusual communication must be reported immediately to the operation coordinator.

9) Device Security

To protect sensitive data and maintain the integrity of icandance's digital operations, all staff, volunteers, and contractors must adhere to the following device security protocols:

- **Password Protection:** All devices used for icandance work, including laptops, tablets, and mobile phones, must be protected with a strong password, biometric login, or PIN. Passwords must comply with the organisation's password policy.

- **Automatic Locking:** Devices must be set to automatically lock after a period of inactivity (recommended: 5 minutes or less). This prevents unauthorised access when the device is unattended.

- **Encryption:** All devices storing or accessing sensitive icandance data must have full-disk encryption enabled. This ensures that data remains protected even if the device is lost or stolen.

- **Software and System Updates:** Operating systems, browsers, antivirus programs, and all relevant software must be regularly updated. Where possible, enable automatic updates to reduce vulnerability to known security threats.

- **Antivirus and Security Software:** Approved antivirus and anti-malware software must be installed and kept up to date. Regular scans should be scheduled, and alerts should be reported to the IT lead or designated person.

- **Prohibited Use of Public Wi-Fi:** Do not access or share sensitive data when connected to unsecured public Wi-Fi (e.g., libraries, cafes, airports). If remote work is necessary, use a secure personal hotspot.

- **Device Disposal:** Before disposing of any device that has been used for icandance work, ensure all data is securely wiped using appropriate data erasure tools or professional services.

- **Lost or Stolen Devices:** Any device containing icandance data that is lost or stolen must be reported immediately to senior leadership so that appropriate incident response and data protection actions can be taken.

10) Cloud Storage and Data Backup

To ensure data security and business continuity, icandance adheres to the following standards for digital storage and backups:

- **Secure Cloud Storage:** All sensitive data, including personal information of dancers, staff, and volunteers, must be stored in secure, password-protected cloud environments (e.g. Microsoft 365). Access to cloud-based documents and folders is managed through role-based permissions to ensure that only authorised personnel can access specific types of data.

- **Encryption and Access Control:** All cloud-stored data should be encrypted at rest and in transit. Access must be protected by strong passwords and two-factor authentication (2FA), and all user access permissions should be reviewed quarterly by the CEO.

- **Data Backups:** Important files and documents must be backed up regularly, at least once per week, to a secure, encrypted backup system. A monthly full-system backup will also be maintained. Backups should be stored in a separate secure cloud location or encrypted external SSD (kept in a safe place) and tested periodically to ensure recoverability.

- **Data Retention and Deletion:** Personal data relating to dancers must be deleted from all systems seven years after the individual has left icandance, unless legal or safeguarding requirements dictate otherwise.

- **Data Transfer and Sharing:** Any transfer of files from cloud storage to external systems or individuals must be logged, encrypted, and shared only through secure, approved methods (e.g. password-protected links with expiration dates).

11) Staff Training and Awareness

To ensure all members of icandance understand and implement secure data practices, the following training protocols are in place:

- **Induction Briefings:** All new volunteers will be introduced to the charity's cybersecurity policy during their induction and part of the icandance handbook, including safe data handling and communication practices.

- **Annual INSET Day Training:** A mandatory cybersecurity refresher will be delivered to all staff and volunteers during the September INSET day. This includes updates on emerging threats, phishing awareness, and secure data handling.

- **Leadership Requirements:** All **senior leads and operation coordintor** must complete certified **Cybersecurity and GDPR training via Educare every 2 years**. This ensures compliance with legal obligations and supports best practice in safeguarding personal data.

- **Refresher and Ongoing Learning:** An **annual refresher** will be provided to all staff and volunteers. This may include:
  - Training videos (e.g., from the NCSC or a verified provider)
  - Scenario-based discussions
  - A short quiz or checklist to confirm understanding

- **Advanced Training:** Advanced-level cybersecurity and data protection training will be provided to designated data leads or system administrators.

- **Incident Awareness and Reporting:** Staff are encouraged to report **any suspicious emails, links, or potential data breaches immediately** to the Designated Safeguarding Lead or operation coordinator. A "See Something, Say Something" approach will be promoted

12) Incident Response

In the event of a data breach or suspected breach, the following steps must be taken promptly to minimise harm and ensure compliance with UK GDPR:



1) Identify

- All team members must report any suspected data breaches immediately to Juliet Diener at juliet@icandance.org.uk
- A breach may include: loss of personal data, unauthorised access to systems, or accidental disclosure.
- Log the date, time, and initial details of the incident for further investigation.

2) Contain

- The responsible technical lead (or staff member) must act to limit the scope of the breach.

1. Examples: disconnect affected devices from the network, revoke access rights, secure physical documents.

- Reset any compromised passwords and disable shared links if applicable.

3) Notify

- If the breach poses a high risk to individuals (e.g. personal or health information), the affected individuals must also be notified in a clear and timely manner.
- Internal notification must be made within 2 hours of identifying the breach.
- If the breach involves high-risk personal data, we will report to the ICO within 72 hours of becoming aware of it, as per UK GDPR Article 33.

4) Investigate

- A formal investigation will be carried out by our IT support, supported by relevant team member.
- Includes: cause analysis, scale of data loss, impact assessment, and actions taken.
- A written incident report will be submitted to the Senior Leadership Team and Trustees.
- Outcomes of the investigation may trigger training updates, technical changes, or policy reviews.

5) Review and Follow-up

- All breach incidents will be documented and reviewed annually by the senior leadership team.
- Lessons learned will be incorporated into future training and system improvements.

13) Regular Review

- This policy will be reviewed annually by senior leadership to ensure it remains effective and up to date with cybersecurity best practices. Trustees will review this policy every three years.
- Review timeline must be tracked and version-controlled in a policy register

Version	Date	Changes Made	Signature
1.0	1/6/2025	Initial policy implementation	Juliet Diener