Release International

Information Security Policy

Introduction

Release International is a Christian organisation and this is expressed in our Ethos Statement and Statement of Faith. The values, attitudes, motivation and relationships of staff and the way the work is achieved is as important as the work itself. We are committed to high standards and we aim to treat everyone in accordance with the Christian values at the heart of our ministry.

As an essential part of Release's work and as an employer, it is necessary to process personal data and/or special categories of personal data (previously referred to as sensitive data). Regulations concerning data protection are in the process of being changed and this policy demonstrates our commitment to comply with regulations concerning the treatment of people's data, whatever their connection with Release. Release is therefore committed to complying with the current Data Protection Act 1998, the European Union General Data Protection Regulation (GDPR), which comes into effect from 25th May 2018 and the new Data Protection Act 2018, when is comes into effect in due course.

Part of this compliance is to ensure the security of information which we hold to protect our supporters and staff and to demonstrate Release understands and applies appropriate guidance and process to recording, storing, processing, exchanging and deleting information. Should this not be achieved Release risks, at worst, the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the ICO. Whilst Release's Data Controller lead is the Director of Engagement UK and Ireland, everyone has a responsibility for ensuring the security of the data they access and process as defined in this Information Security Policy.

This Information Security Policy outlines Release's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the organisation's information systems. Release is committed to a robust implementation of Information Security management and aims to ensure the appropriate confidentiality, integrity and availability of the data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which Release is responsible.

This policy should be read in conjunction with the other policies and documents mentioned within this policy.

This policy applies to all staff, whether full-time, part-time, temporary or permanent and to any consultants working on our behalf. The policy also applies to Trustees and Volunteers in the course of their work in connection with Release. The term staff is used throughout this policy to apply to all of the above.

Aims

- To explain the Information Security of records and data
- To provide a framework for establishing appropriate levels of Information Security for all information systems (including Cloud environments) run by Release; and for computers, storage, mobile devices, networking equipment, software and data contained therein
- To mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems and equipment
- To ensure users are aware of and comply with all current and relevant UK and EU legislation
- To explain key Information Security principles by which a safe and secure information environment can be established for staff, volunteers and any other authorised users
- To ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle
- To establish a process for how staff are trained in relation to this policy
- To establish a procedure for handling any breach in policy
- To establish a procedure for handling complaints regarding this policy
- To establish a process to implement, monitor, evaluate and review this policy.

Privacy Statement

Release's Privacy Statement is a public document which explains why we process personal data, the lawful bases for doing so, retention periods of the data, individuals' rights, how to request personal data held, how to make a complaint and issues relating to data security and breach notification. It also includes full contact details.

Release's Privacy Statement is available on Release's website and by request from the Release office 01689 823491.

Information security principles

Article 5 of the GDPR requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The following information security principles provide overarching governance for the security and management of information at Release:

- Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Information Classification*) and in accordance with relevant legislative, regulatory and contractual requirements.
- Staff with particular responsibilities for information classification (see *Responsibilities*) must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

- All users must handle information appropriately and in accordance with its classification level.
- Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
- Information will be protected against unauthorized access and processing in accordance with its classification level.
- Breaches of this policy must be reported in line with the Data Breach Policy.
- Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual audits and penetration testing.

Legal & Regulatory Obligations

Release International will at all times abide by and adhere to all current UK and EU legislation as well as all applicable regulatory and contractual requirements. This legislation is listed below and includes (but not exhaustively):

Data Protection Act (1998)	Designed to protect personal data stored on computers or in an organised filing system.
General Data Protection Regulation	Reinforces and extends data subjects' rights as laid out in the Data Protection Act (1998) and provides additional stipulations around accountability and governance.
The Computer Misuse Act 1990	Defines offences in relation to the misuse of computers.
Defamation Act 1996	Exists to protect a person or an organisation's reputation from harm.
Obscene Publications Act 1959 &1964	The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" and includes extreme violence and torture.

Information Classification

The following table provides a summary of the information classification levels that have been adopted by Release and which underpin the seven principles of information security defined in this policy. These classification levels explicitly incorporate the General Data Protection Regulation's definitions of Personal Data and Special Categories of Personal Data, as laid out in the Data Protection Policy, and are designed to cover all areas of information.

Security Level	Definition	Examples
1. Confidential	Normally accessible only to specified members of Release staff. Should be held in an encrypted state outside Release systems.	GDPR-defined special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record)
2. Restricted	Normally accessible only to specified members of Release staff trustees and volunteers	GDPR-defined Personal Data (information that identifies living individuals including home / work

Security Level	Definition	Examples
		address, age, telephone number, photographs), Committee business papers, draft reports and minutes
3. Internal Use	Normally accessible only to members of Release staff, trustees and volunteers	Internal correspondence, working papers, prayer requests and information held under license
4. Public	Accessible to all members of the public	Annual accounts, impact reports, magazines and other promotional material.

Suppliers

All of Release's suppliers will abide by Release's Information Security Policy, or otherwise be capable of demonstrating corporate security policies providing equivalent assurance. This particularly applies to suppliers who have access for support or audit purposes to Release systems and data.

Where Release uses Cloud services, Release retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. Release will also bear the responsibility for contacting Information Commissioner's Office concerning the breach, as well as any affected individual.

This leads to the following stipulations:

- All providers of Cloud services to Release must demonstrate the policy and processes by which they themselves are compliant with GDPR.
- Cloud services used to process personal data will be expected to have systems which meet ISO27001 certification, with adherence to the standard considered the best way of a supplier proving that it has met the GDPR principle of privacy by design, and that it has considered information security throughout its service model.

Requirements

For the avoidance of doubt, the Information Security Policy requires that:

- Individuals must ensure that as far as is possible no unauthorised person has access to any data held by Release.
- Individuals must ensure that physical security measures are properly used.
- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to the Release (this includes the deliberate or negligent introduction of viruses or other malware).
- Individuals will be given access passwords to certain computer systems, these must adhere good password practice (refer to Director of Resources DoR), not be disclosed to other members of staff or volunteers, they should not be written down and they must be changed regularly.
- If access is required to your Z: drive, for example if you are off sick, a manager should make a request to the DoR who will arrange temporary access.

- Any individual found to be storing large numbers of personal files, especially large files such as photographs or videos may be asked to remove them or in some circumstances be the subject of disciplinary action.

Security

Only Release owned computers are allowed to be connected to the Release network. Personal devices and visitors may access the Release (Guest) WiFi network.

Access to data held on the systems is minimised by restricting physical access to the Release office. Staff should ensure that external doors and internal lock-controlled access doors are closed properly and that entry codes are kept secure. Doors and windows must be secured at all times when the office is left unattended.

Access to individual systems and data drives areas will only be granted by the "owners" of that area.

Computers must not be left unattended with screen unlocked when logged in to the network (hit 'Windows key' + L to lock). When leaving their place of work staff must ensure they have logged off and closed down the computer correctly.

Data Storage

Storage of data on the internal C: drive is discouraged and all users are requested not to store files on the C: drives as, in the event of failure, all data stored on that drive would be lost as it not backed up.

All information related to Release business is to be stored on the personal network drive (the Z:\ drive) or on the Shared drive or other network drives. This is a secure storage area which is regularly backed up and is therefore resilient to failure.

All documents and files should be given clear and descriptive titles that will help others to understand what is contained within them. Where relevant documents should have a date and version number clearly included.

Information which is no longer required in line with the Data Retention Policy should be promptly disposed of by deletion or destruction. Unless an audit record of versions is explicitly required previous versions of documents should be destroyed when the new version is created.

Personal data as defined under GDPR must not be stored on a removable drive, 'USB memory sticks or CD/ DVD (unless to be retained securely in the office for archive purposes).

Document Handling

All paper documents containing personal data should be securely locked away when no longer being used. Paper documents containing personal data no longer required should be shredded.

Mobile Devices and Home Workers

Laptops must not be left unattended whilst they are located outside of the office or staff member's home.

When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it. Care must be taken to avoid being overlooked whilst using equipment in any public area.

Staff using mobile phones or other Personal Digital equipment which can access Release data (including emails) are responsible for safekeeping and security. Security lock and pin protection must be used where available to protect the device and any stored data.

If a mobile device is lost or stolen, staff must report the loss to the network provider and ask for the mobile device to be disabled so that it can no longer be used. If it is enabled for access to Release systems they should also contact Utilize and have their password changed immediately.

Notify the local Police station of the loss.

Personal Data Breaches

Any security breach of Release's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes Release's Data Protection Policy, and may result in criminal or civil action against Release.

All current staff, volunteers and other authorised users will be informed of the existence of this policy and the all related policies, codes of practice and guidelines.

Any security breach should be immediately reported to the Data Protection Officer, who will notify the ICO, and will be handled in accordance with the Data Breach Policy.

Complaints about Data Security

Release has a formal Supporters' Complaints Procedure which is available publicly on Release's website. This includes the right to make a complaint to UK regulatory authorities if necessary or if Release has been unable to resolve the issue to the complainant's satisfaction.

This Procedure should be used as needed by supporters, prospective supporters, volunteers, prospective volunteers, suppliers, prospective employees, or our International partners. Staff who have a complaint about data security should raise it through Release's Grievance Policy.

Any complaints which are received of a compliance nature, including Data Protection, are reported to the Board of Trustees through the UK Engagement Committee at quarterly Board meetings.

Training

All staff receive Induction relevant to their role and Information Security is included within this. Further training on Information Security will be provided as required and relevant to specific roles.

Compliance and Disciplinary Action

If a member of staff is considered to have breached this policy it will be dealt with in accordance with Release's Disciplinary Policy.

Complaints

Any complaints about the handling of matters relating to this policy are to be made in line with Release's Grievance Policy.

Implementation, Monitoring, Evaluation and Review

This policy will be implemented by The Director of Engagement UK and Ireland who will monitor, evaluate and review its effectiveness. The policy will be reviewed every two years or sooner as appropriate or if there are legislative changes.

David Binns May 2018
Review May 2020