DATA SECURITY POLICY

Version number:	1.0	**Ref:**	IG.4
Reviewer:	Fiona Green Policy Officer	**Date:**	April 2021
Lead SMT member:	Clare Evans Head of Volunteer Services Data Protection Lead and Caldicott Guardian	**Date:**	April 2021
Considered by SMT:	Yes	**Date:**	April 2021
Approved by:	Alan Hopley Chief Executive	**Date:**	May 2021
Board approval required:	V1.0	**Date**	May 2021
Updates included	1.0 Based on template provided by Care Provider Alliance		
Next review due	May 2022		

1. Introduction

This Data Security Policy is Voluntary Norfolk's (hereafter referred to as "us", "we", or "our") policy regarding the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 2018, Health & Social Care Act 2012, and the Common Law duty of confidentiality). It should be read and considered in conjunction with the Voluntary Norfolk Data Protection Policy and forms part of a suite of policies and procedures that document how Voluntary Norfolk protects the confidentiality, security and integrity of the personal data we process.

The purpose of this policy is to outline how we prevent data security breaches and how we react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

This policy covers:

- Physical Access
- Digital Access

- Access Monitoring
- Data Security Audit
- Loss, destruction or damage by accident or incident
- Third party service providers
- Data Security Breach

This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

This policy applies to all current and former members of staff, including employees, volunteers, trustees, casual workers, agency workers, apprentices, contractors and consultants whether temporary or permanent.

2. Definitions

In this policy, the following words and phrases have the following meanings:

Consent - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

Data subject - a living identified or identifiable individual about whom Voluntary Norfolk holds personal data.

Personal data - any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data, i.e. where all identifying particulars have been removed.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

Service user - includes any network member organisation and their representatives, any client or other customer of the charity's activities, services, projects or divisions and all visitors to Voluntary Norfolk premises.

Special categories of personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject's sex life or sexual orientation.

Staff – includes current, former and potential employees, volunteers, trustees, casual workers, agency workers, apprentices, contractors and consultants whether temporary or permanent.

3. Physical access

Physical access to records shall only be granted on a strict 'Need to Know' basis.

Staff must retain personal and confidential data securely in locked storage when not in use and keys should not be left in the barrels of filing cabinets, drawers and doors.

All offices, when left unoccupied, must be locked unless all personal and confidential information has first been cleared from work stations/desks and secured in locked storage.

Staff must assume that a clear desk policy applies unless agreement to the contrary has been given for a limited time period for a specific reason by the relevant Line Manager or Service Lead – see Voluntary Norfolk Clear Desk and Screen Policy.

The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information and is stored in the Data Security Folder on the SMT drive. Each physical storage location must be risk assessed to ensure that the data is properly secured. This risk assessment forms part of the IAR.

A record will be kept of who has access to each physical storage location. This record is maintained and updated by the Data Protection Lead (DPL), supported by the Head of Resources and Facilities (HRF), and is kept in the Data Security folder on the SMT drive.

An audit will be completed at least annually to ensure that information is secured properly and that access is restricted to those who have a legal requirement to use the information. The details of this audit are outlined in the Data Security Audit section below.

4. Digital access

Digital access shall be granted using the principle of 'Least Privilege'. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.

We will ensure that each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.

Each system is the responsibility of the Service Lead or accountable officer who will ensure a record is kept of all users given access to the system. This record is maintained and updated by the Service Lead, supported by the Data Protection Lead (DPL) and is kept in the Data Security folder on the SMT drive.

In the instance that there are changes to user access requirements, these can only be authorised by the Service Lead or the DPL.

The IAR will contain the location of all confidential and sensitive personal information which is digitally stored and the Service Lead or accountable officer has responsibility for ensuring it remains accurate and up to date, with support from the DPL.

Voluntary Norfolk and all its departments and services will follow robust password management procedures and ensure that all staff are trained in password management. See Voluntary Norfolk Password Management Policy.

As soon as an employee leaves, all their system logons are revoked.

As part of the employee termination process the Service Lead or Line Manager is responsible for the removal of access rights from the computer system – this should be included in the employee's exit strategy and return of equipment as detailed in the employee's confirmation of end date.

Folders associated with these access rights will be archived unless identified within a work group.

When not in use all screens will be locked and a clear screen policy will be followed – see Voluntary Norfolk Clear Desk and Screen Policy.

Voluntary Norfolk's ICT requirements are currently contracted to PremierLinks Ltd.

5. Access monitoring

The DPL and HRF will review all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons which are identified are disabled immediately and deleted unless positively reconfirmed.

Regular compliance checks will ensure that this policy is being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

Areas considered in the compliance check include whether:

- Allocation of administrator rights is restricted;
- Access rights are regularly reviewed;
- Whether there is any evidence of staff sharing their access rights;
- Staff are appropriately logging out of the system;
- The Voluntary Norfolk Password Management Policy is being followed;
- Staff understand how to report any potential security breaches or concerns.

6. Data security audit

Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls.

Audits of security and access arrangements within each area are to be conducted on an annual basis.

Audits will be carried out as required by some or all of these methods:

- Unannounced spot checks to random work areas;
- A series of interviews with management and staff, where a department or area of the organisation have been identified for a confidentiality audit. These audits will be carried out by the Service Lead with support from the DPL;
- Electronic reports from ICT contractor, currently Premier Links or from other internal monitoring;

The following checks are representative of activities that may be included in data security audits:

- That the Information Asset Register has been reviewed, updated and signed off;
- That the Record of Processing Activities has been reviewed, updated and signed off;
- Failed attempts to access confidential information;
- Repeated attempts to access confidential information;
- Access of confidential information by unauthorised persons;
- Previous confidentiality breaches, incidents and investigations, including any disciplinary action taken;
- Staff awareness of policies and guidelines concerning confidentiality and data security and their understanding of their responsibilities with regard to confidentiality;
- Appropriate communications with service users;
- Appropriate recording and/or use of consent forms;
- Appropriate allocation of access rights to confidential information, both hardcopy and digital;
- Appropriate staff access to physical areas;
- Storage of and access to filed hardcopy service user notes and information;
- Use of the correct processes to securely transfer personal information by post, fax or email as appropriate;
- Appropriate use and security of desk and mobile devices in open areas;
- Security applied to PCs, laptops and mobile electronic devices;
- Evidence of secure waste disposal;
- That appropriate data transfer and sharing arrangements are in place;
- Security and arrangements for recording access applied to manual files both live and archive, e.g. storage in locked cabinets/locked rooms.
- Appropriate staff use of computer systems, e.g. little or no personal use, no attempting to download software without authorisation, only approved use of social media, attempted connection of unauthorised devices.

7. Loss, destruction or damage by accident or incident

Personal data must 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.

Voluntary Norfolk takes the security of personal data seriously. We have implemented and will maintain safeguards which are appropriate to the size and scope of our business, the amount of personal data that we hold and any identified risks. This includes encryption and pseudonymisation of personal data where appropriate. We have also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of our processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner.

We regularly test and evaluate the effectiveness of our technical and organisational safeguards to ensure the security of our processing activities.

In turn, staff are responsible for protecting the personal data that we hold, and must implement reasonable and appropriate security measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage. Staff must be particularly careful in protecting special categories of personal data and criminal records personal data. You must follow all procedures, and comply with all technologies and safeguards, that we put in place to maintain the security of personal data from the point of collection to the point of destruction.

8. Third party service providers

Where Voluntary Norfolk uses third-party service providers to process personal data on our behalf, additional security arrangements will be implemented in contracts with those third parties to safeguard the security of personal data. Staff can only share personal data with third-party service providers if they have been authorised to do so and provided that certain safeguards and contractual arrangements have been put in place, including that:

- the third party has a business need to know the personal data for the purposes of providing the contracted services
- sharing the personal data complies with the privacy notice that has been provided to the data subject (and, if required, the data subject's consent has been obtained)
- the third party has agreed to comply with our data security policy and has put adequate measures in place in ensure the security of processing
- the third party only acts on our documented written instructions
- a written contract is in place between Voluntary Norfolk and the third party that contains specific approved terms
- the third party will assist Voluntary Norfolk in allowing data subjects to exercise their rights in relation to data protection and in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments

- the third party will delete or return all personal data to Voluntary Norfolk at the end of the contract
- the third party will submit to audits.

Before any new agreement involving the processing of personal data by a third-party service provider is entered into, or an existing contract is amended, a Data Protection Impact Assessment must be completed in line with Voluntary Norfolk's Data Protection Impact Assessment Procedure.

Voluntary Norfolk has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.

9. Data security breach

Voluntary Norfolk takes the issue of real or suspected data breach seriously. If you know or suspect that a personal data breach has occurred, you must immediately notify your Service Lead/Line Manager/Volunteer Coordinator who will liaise with the DPL for further investigation in line with Voluntary Norfolk's Data Breach Procedure and Response Plan.

10. Training

During their induction each staff member who requires access to confidential information for their job role will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised both in Voluntary Norfolk as a whole and in their particular team and/or service.

Each staff member who requires access to digital systems for their role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access. Each staff member is required to read this Data Security Policy and must not access digital systems until they and their Service Lead, Line Manager or Volunteer Coordinator are comfortable that they understand the requirements of this policy.

11. Non-compliance

Any potential infringement of the above may constitute a breach and will be thoroughly investigated. Any breach is considered a serious matter.

Employees who are found to be in contravention of this policy may be subject to disciplinary action in accordance with the Voluntary Norfolk disciplinary policy. Should a breach amount to a gross misconduct offence under Voluntary Norfolk's disciplinary policy, this could lead to summary dismissal.

Volunteers who are found to be in contravention of this policy may be subject to the problem solving procedure in accordance with the Voluntary Norfolk Volunteer Policy. Should a significant breach be confirmed, this could lead to termination of volunteer agreements.

For those who have a different relationship with Voluntary Norfolk, should a breach be confirmed, they may find their relationship terminated and, even if this involvement is no longer current, we may consider taking legal action.

12. Key contacts & responsibilities

The Trustees have overall responsibility for ensuring implementation, communication of and adherence to this policy and will periodically appraise the effectiveness of the policy.

On a day to day basis this responsibility is delegated to the Chief Executive, Alan Hopley, who is also our Senior Information Risk Owner (SIRO). His key responsibilities as SIRO are:

- To manage, assess and mitigate information risks within Voluntary Norfolk;
- To represent all aspects of information and data protection and security to senior management and drive engagement in data protection at the highest levels of the organisation.

Our designated Data Protection Lead (DPL) is Head of Volunteer Services, Clare Evans. Her key responsibilities as DPL are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;
- To define our data protection policy and work with department and service leads in the development, implementation and monitoring of associated procedures and processes.
- To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.
- To monitor information handling to ensure compliance with the law and Voluntary Norfolk policies.
- To liaise with the SIRO to ensure that sufficient resources are provided to support policy requirements and any associated local procedures
- To liaise with the SIROs, DPOs and DPLs of organisations that act as data controllers for services or projects where Voluntary Norfolk is contracted to operate as a data processor.

Any queries or concerns regarding the policy can be addressed to the DPL via:

Email: clare.evans@voluntarynorfolk.org.uk

Telephone: 07910 630006

Correspondence by Post: St Clements House, 2-16 Colegate, Norwich, NR3 1BQ

Our Head of Resources and Facilities is Julia Creusson who can be contacted as follows:

Email: julia.creusson@voluntarynorfolk.org.uk

Telephone: 07471 998343

Correspondence by Post: St Clements House, 2-16 Colegate, Norwich, NR3 1BQ

Premier Links are Voluntary Norfolk's IT contractor and can be contacted as follows:

Email: support@premierlinks.co.uk

Telephone: 01692 403036

13. Data protection

In the implementation of this policy, Voluntary Norfolk may process personal data and/or special category personal data collected in accordance with our Data Protection policy. Data collected from the point at which this policy is invoked will only inform the charity for the benefit of implementing this policy. All data is held securely and accessed by, and disclosed to, individuals only for the purposes of this policy.

Inappropriate access or disclosure of personal data constitutes a data breach and should be reported in accordance with our UK GDPR and data protection policy immediately. For current employees this conduct may amount to a gross misconduct offence under Voluntary Norfolk's Voluntary Norfolk following investigation this may be terminated and even if your involvement with Voluntary Norfolk is no longer current we may consider taking legal action.