DATA PROTECTION POLICY

Version number:	3.1	**Ref:**	IG.3
Reviewer:	Fiona Green Policy Officer	**Date:**	May 2021
Lead SMT member:	Clare Evans Head of Volunteer Services, Data Protection Lead	**Date:**	May 2021
Considered by SMT:	Yes	**Date:**	May 2021
Approved by:	Alan Hopley Chief Executive	**Date:**	June 2021
Board approval required:	Yes	**Date**	July 2021
Updates included	2.0/1/2 Based on CBR template, reformat, update contact 3.0 Separation of policy and procedure – policy based on template provided by Care Provider Alliance 3.1 General review and update, change from GDPR to UK GDPR		
Next review due	July 2022		

1. Introduction

The Policy Officer and Data Protection Lead have been working with the Governance team at Norfolk CCG to develop a suite of data security and protection policies, procedures and guidelines to ensure compliance with The Data Security and Protection Toolkit - an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

This Data Protection Policy is the overarching policy for data security and protection for Voluntary Norfolk (hereafter referred to as, "us", "we", or "our").

The purpose of this Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulation (2016) which has been incorporated into UK data protection law following Brexit as UK GDPR, the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation.

Voluntary Norfolk recognises data protection as a fundamental right and embraces the principles of data protection by design and by default.

This policy covers

- Our data protection principles and commitment to common law and legislative compliance
- Data protection by design and by default.

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 our workforce, including employees, volunteers, trustees, casual workers, agency workers, apprentices, contractors and consultants whether temporary or permanent. As a member of our workforce, you are yourself a data subject and you may also process personal data on Voluntary Norfolk's behalf about other data subjects. This policy should be read and interpreted accordingly; it sets out what we expect from you and explains the rules governing the processing of personal data. You must always comply with it.

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 that 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. Principles

3.1 We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

3.2 We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the UK General Data Protection Regulation and all other relevant legislation.

3.3 We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

3.4 Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Data Subject Access and Other Rights Requests Policy and Procedure. We ensure that it is as easy to withdraw as to give consent.

3.5 We will undertake annual audits of our compliance with legal requirements.

3.6 We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
- Processed in a manner that ensures appropriate security of the personal data.

3.7 We uphold the personal data rights outlined in the UK GDPR;

- The right to be informed;
- The right of access;

- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

3.8 Due to our size and as we do not process special categories of data on a large scale, we have determined that we are not required to have a Data Protection Officer (DPO). Nonetheless, to ensure that every individual's data rights are respected and that there is the highest levels of data security and protection in our organisation, we have appointed a senior member of staff to the role of Data Protection Lead. The Data Protection Lead reports directly to the Chief Executive and is supported with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

4. Underpinning policies & procedures

This policy is underpinned by the following:

- Data Quality Policy – details commitment to ensure the accuracy of records, identification and correction of errors and the overarching standards individual services and departments must aim to achieve;

- Record Keeping and Handling Policy – details commitment to ensure transparency in the management of records from creation to disposal including information handling and the overarching standards individual services and departments must aim for;

- Data Subject Access and Other Rights Requests Policy – provides guidance on making and responding to subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share personal data;

- Data Retention and Destruction Policy – outlines to commitment to only retain personal data in a form which permits identification of data subjects for as long as is strictly necessary for the purposes for which the personal data are processed.

- Data Security Policy – details commitment to ensure the security of data;

- Data Breach Policy, Procedure and Response Plan – provides clear guidance on the reporting of a suspected or actual data breach and the commitment to a coordinated response.

- Clear Desk and Screen Policy – details commitment to protect data;

- Business Continuity Plan –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation;

- Staff Confidentiality Code of Conduct - provides staff with clear guidance on the disclosure of personal information.

- Volunteer Policy – provides guidance for volunteers on the disclosure of personal information.

- Privacy Policy and associated Privacy Notices – provide information on how personal data will be collected, stored and processed by Voluntary Norfolk and individual services and departments.

- IT Policy – provides guidance and procedures on network security, password management and cyber security.

- Disciplinary Policy – provides guidance on how staff found to be in breach of this policy will be reprimanded

5. Data protection by design & by default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

Adherence to Voluntary Norfolk's Data Protection Impact Assessment Procedure provides evidence that an appropriate risk assessment of data protection compliance and security certification has been undertaken, and ensures that consideration has been given to the data protection implications of any project or activity and the application of all relevant data protection principles before personal data processing takes place.

6. 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 procedure. Should a breach amount to a gross misconduct offence under Voluntary Norfolk's disciplinary procedure, 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.

7. 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

8. 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 disciplinary procedure and could lead to summary dismissal; if you have a different relationship with 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.