General Data Protection Regulation (GDPR) and Data Protection Act (2018) Policy

Current Version	**1.4**
Policy Author	Michael Daley
Date Written	December 2021
Date Approved by SLT/CEO	31 January 2022
Implementation Date	31 January 2022
Description of Change	Revisions required to demonstrate compliance with the NHS DSPT Toolkit.
Next Review Date	**Annual – January 2023**

Version History/Information	
Version	Previously named Data Protection Policy v1.0
Author	Graham Barker
Implemented	10th May 2017
Description of Changes	Policy rewritten following new GDPR regulations introduced 26 May 2018.
Version	1.0
Author	Rob Kendall
Approved	August 2018
Implemented	4 September 2018 (review by Dec 2018)
Description of Changes	Cross referenced with other policies. Updated to include Section 15 Safeguarding Children, young people and adults and covers exemptions to GDPR/DPA when there is a safeguarding concern. Subsequent sections renumbered.
Version 1.1/1.2	Link to Right to Erasure policy added, plus clarification of 'certain circumstances' in 6. Included section on lawful basis for processing
Author	Rob Kendall
Date Approved by SLT/CEO	4 December 2018
Implemented	4 December 2018
Version	1.3
Author	Garry Besford
Implemented	September 2019
Description of Changes	Disclosure Policy amalgamated into GDPR Policy

This policy is to be read in conjunction with the below Daisy Chain Policies:

- Safeguarding Children Policy
- Safeguarding Adults Policy
- CCTV Policy
- Confidentiality Policy
- Data Subject Access Request Policy
- Right to Erasure Policy

General Data Protection Regulation (GDPR) & Data Protection Act (2018) Policy

1. Introduction

This document sets out the obligations of Daisy Chain with regard to data protection and the rights of the people with whom it works in respect of their personal data under both the General Data Protection Regulation (herein GDPR), which was introduced on 25th May 2018 and the Data Protection Act 2018.

This policy shall aim to set out the procedures which are to be followed by Daisy Chain, its trustees, staff and volunteers. Agents working on behalf of Daisy Chain are also required to follow this policy when handling and processing personal data.

Daisy Chain views the correct and lawful handling and processing of personal data as key to its success and dealings with its employees, volunteers and third parties. Daisy Chain will ensure that it handles all personal data correctly and lawfully.

2. Policy Statement

Daisy Chain is committed to a policy of protecting the rights and privacy of individuals in accordance with the GDPR and Data Protection Act 2018.

Daisy Chain needs to process certain information about its staff, volunteers, service users and other individuals and organisations it has dealings with, for administrative and legal purposes.

To comply with the law, the information about these individuals must be collected, processed and used fairly under the terms that have been agreed. All information is to be stored safely and securely and must not be disclosed to any third party unlawfully.

This policy applies to all trustees, employees and volunteers at Daisy Chain. Any breaches of the GDPR, Data Protection Act 2018 or the GDPR policy may be considered to be an offence. In this event, Daisy Chain's disciplinary procedures may be applied. All breaches are to be recorded by the Data Protection Officer and may in turn be reported to the Information Commissioner's Office for an external investigation to be undertaken.

As the data controller, Daisy Chain shall be responsible for, and will demonstrate continued compliance with the principles set out in Article 5 (2) of the GDPR. Therefore, as a matter of good practice, other agencies and individuals working with, or on behalf of Daisy Chain who have access to any personal information will be expected to read and comply with this policy.

3. Responsibilities

a. **Chief Executive Officer** – Will uphold the policy and provide authorisation for any investigations to take place should the relevant procedures not be adhered to

b. **Data Protection Officer** – Has statutory responsibilities in relation to Data Protection and the upholding of policies and procedures

c. **Senior Leadership Team** – Will ensure that teams have access to, understand and adhere to the policy and the associated GDPR regulations. They will also ensure Data Protection spot checks are completed by either themselves or their Managers.

d. **Managers and coordinators** – Will ensure that all staff are aware of and have read the policy. They will also complete Data Protection spot checks as instructed by SLT.

e. **Staff** – Will adhere to the policy and report any potential breaches to the Data Protection Officer immediately.

4. Data Protection Act 2018 (DPA) and GDPR

The GDPR officially came in to effect on 25th May 2018 following a two-year transitionary period. DPA 2018 is the UK's third generation of data protection law replacing the 1998 and 1984 acts and the Access to Personal Files Act 1987.

The GDPR has direct effect across all EU member states. This means that organisations will still have to comply with the GDPR and in most instances it will apply. However, the GDPR does give member states a limited opportunity for how it applies in their country. It is therefore important that the principles of GDPR and DPA 2018 are applied together.

GDPR has been introduced to give the data subject more control over their personal information and the reasons why it is used. Data processors must be clear on the lawful basis for processing information. There are 6 lawful reasons for processing which can be found in annex A.

5. Daisy Chain's responsibility under the GDPR

Daisy Chain as a charity is the registered data controller under the GDPR. This means that as an organisation, Daisy Chain has the overall control over the purpose for which, and the manner in which, personal data are processed.

A Data Protection Officer (DPO) has been appointed who is responsible for day to day data protection matters and for developing specific guidance notes on data protection issues for Daisy Chain.

Daisy Chain will, through appropriate management and the use of appropriate controls adhere to the following in regards to our use of personal data and special category personal data:

- Provide up to date privacy notices to data subjects.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Ensure the quality and accuracy of information when collected or received and during its use.
- Apply checks to determine the length of time information is retained.
- Take appropriate technical and organisational security measures based on risks to data subjects.
- Not transfer outside the EEA without suitable safeguards.
- Ensure that any information incidents are reported and where appropriate the data subject and the Information Comissioners Office.

- Mitigate risks to the data subjects in the event of an information incident using an appropriate data breach policy.
- Ensure that the rights of our data subjects can be properly exercised.

These rights are outlined further in Section 6.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

In addition, we will ensure that:

- There is someone with specific responsibility for data protection in the organisation. The post responsible for data protection is CEO.
- Organisational information and in particular privacy risks are risk assessed, documented and controlled.
- Everyone managing and handling personal data and special category personal data understands that they are responsible for following good Information Governance / Assurance practice and for complying with the data protection legislation.
- Everyone managing and handling personal data and special category personal data is appropriately trained and supervised to do so.
- Queries about processing personal data and special category personal data are promptly and courteously dealt with within the requirements of the data protection legislation.
- Data sharing and processing is carried out under an appropriate written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All employees and volunteers are to be made fully aware of this policy and their duties and responsibilities under it. All employees and volunteers will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

6. Individuals rights under the GDPR

The GDPR provides individuals with rights as to how Daisy Chain uses the information that has been collected. They are:

a. The right to be informed – Individuals have the right to be informed about the collection and use of their personal data by Daisy Chain. This is a key transparency requirement under the GDPR.

Individuals must be provided with information including: Daisy Chain's purposes for processing their personal data, the retention periods that are employed by Daisy Chain, and who it will be shared with.

b. The right of access – Individuals whose data is processed by Daisy Chain have the right to access their personal data. This is sometimes referred to as subject access.

Should an individual make a request to see their stored data, they can do so both verbally or in writing. Under the guidelines of the GDPR, Daisy Chain must provide the information that has been requested within one month.

Further information on an individual's right of access can be found in the Subject Access Request Policy.

c. The right to rectification – An individual can make a request for their data to be corrected should it be inaccurate, or for it to be completed if it is incomplete. As with a subject access request, Daisy Chain will respond to such requests within one calendar month.

d. The right to erasure (also known as 'the right to be forgotten') – The GDPR gives a right for an individual to have personal data erased. This is not absolute and can only be applied in certain circumstances (for more information please see 'Right to Erasure Policy').

e. The right to restrict processing – Under the GDPR, individuals have the right to request the restriction or suppression of their personal data. In these circumstances, if processing is restricted, personal data can be stored but not used. This is not an absolute right for the individual and can only be used in certain circumstances. In the event that a request is received, contact the Data Protection Officer.

f. The right to data portability – This allows individuals the right to receive any personal data they have provided to a controller (in this instance to Daisy Chain) in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller, i.e. Microsoft Word/Excel.

g. The right to object – GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. For instance, individuals have an absolute right to stop their data being used for direct marketing.

h. Rights in relation to automated decision making and profiling - The UK GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

7. Children and the GDPR

Children require particular protection when their personal data is being collected and processed as they may be less aware of the risks involved. When processing the personal data of a child, it should remain the intention to protect them from the outset.

There must be a clear and understood lawful basis for processing the personal data of a child. It is possible to use consent as the lawful basis however this may not be the most suitable. Data Protection Impact Assessments (DPIA) (see Annex

D) should be used as a matter of good practice, as a means to assess and mitigate the risks to children.

Children have the same rights as adults over their personal data and how it is used. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

8. Reporting a suspected Data Breach

Under the GDPR and DPA 2018, a data breach is defined as:

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

This includes breaches that are the result of both accidental and unlawful causes. It also means that a breach is more than just about losing personal data.

For example, personal data breaches can include:

a. access by an unauthorised third party;
b. deliberate or accidental action (or inaction) by a controller or processor;
c. sending personal data to an incorrect recipient;
d. computing devices containing personal data being lost or stolen;
e. alteration of personal data without permission; and
f. loss of availability of personal data.

When a potential data breach has occurred, the Data Protection Officer must be made aware without delay.

The DPO will then establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there is a risk then the DPO will submit a report to the Information Commissioner's Office within a maximum of 72 hours of the breach occurring.

Although not all breaches need to be reported to the Information Commissioner's Office, they do need to be recorded. It is therefore expected that staff will notify the DPO or a member of the Senior Leadership Team if they feel there has been a breach. This will allow for investigations to take place.

9. Key Principles of GDPR

The processing of all data by Daisy Chain must be done so in line with the key principles of the GDPR which are broadly similar to the principles of the Data Protection Act 1998. These principles are:

a. lawfulness, fairness and transparency
b. purpose limitation
c. data minimisation
d. accuracy
e. storage limitation
f. integrity and confidentiality
g. accountability.

An explanation of the key principles can be found in **annex B**

10. Security of Data

Daisy Chain discourages the removal of personal information from it's sites and premises but understands that this is not always possible. Therefore, where it is deemed appropriate to do so, individuals must obtain permission from their Line Manager/SLT. If there is considered to be a risk, the decision will be made by the CEO and/or DPO. All trustees, staff and volunteers are responsible for ensuring that any personal and sensitive information which they hold are kept securely and are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who require it to perform their business duties.

It is the responsibility of the individual using the data to form a judgement based on the sensitivity and value of the information in question, but always consider keeping personal data:

a. in a lockable room with controlled access;
b. in a locked drawer of filing cabinet;
c. if computer based records, password protected; and
d. if prior authorisation has been sought from a member of SLT or the DPO on an encrypted USB device.

Care should be taken to ensure that PCs and associated terminals are not visible except to authorised staff and volunteers.

All passwords are to be kept securely and are not to be shared with any other persons.

PCs are not to be left unattended without being 'locked' first and manual records should not be left where they can be accessed by unauthorised personnel.

11. Security in place to prevent unauthorised access to data

Daisy Chain uses various methods to ensure that the information which it holds is secure. This includes physical and IT related.

Current physical security measures on Daisy Chain sites are:

<u>Day Centre</u>
a. monitored alarm system
b. dead locks on external doors
c. fob controlled magnetic internal doors (all)
d. lockable filing cabinets and drawers
e. 2 x lockable safe
f. enclosed server
g. key safe

<u>Farmhouse</u>
a. monitored alarm system
b. 5 lever locks on external doors
c. minimum of 3 lever locks on internal doors
d. 1 x lockable safe

e. lockable filing cabinets and drawers
f. key safe

Superstore
a. monitored alarm system
b. electronic locks
c. roller shutters
d. lockable filing cabinets and drawers
e. lockable safe
f. minimum of 3 lever locks on internal doors

Daisy Chain also has a secure computer network with up to date virus detection software and firewalls, which requires devices to be kept up to date. Access to the Wi-Fi network is controlled by password. This is not to be provided to any of those accessing the services offered by Daisy Chain.

Daisy Chain's devices will be encrypted and staff must ensure that encryption passwords are not stored with the device under any circumstances to avoid unauthorised access to the machine or any of Daisy Chain's systems.

Computer network policies also require passwords to be updated every three months. This also covers cloud based client management systems. Staff should ensure that passwords are strong and not easily guessable.

Staff must ensure that all computers are only used in safe locations, where sight of screen is minimised; particularly in instances where they are accessing sensitive and personal data. Similarly, where devices are not in use, these should be turned off and locked or stored carefully when not in use.

When sending emails concerning work, Staff must use their Daisy Chain email address at all times so to minimise the risk of data being intercepted. Emails sent via Daisy Chain's email system which contain personal or sensitive information must be checked to ensure they are being sent to the correct recipient. Any personal information should be password protected and communicated with the recipient separate to that email thread – For example, by a separate email or via telephone call.

12. Disaster Recovery

In the event of an IT related failure, regular data backups are undertaken to try and reduce any potential impact on the organisation and its data subjects.

Currently Daisy Chain uses various on and off-site methods to back up data which is dependent on which server/operating system is being used. They are:

a. TimeMachine (On site) – Used to back up both Apple Servers, and all network share data backs up every hour.
b. Windows Backups (On site) – Used to back up Sage applications each day;
c. Crashplan (Off site) – Creates a backup of all of the above each night.

TimeMachine has an 8tb storage capacity and will overwrite data once the disk is full. Once this happens, the oldest backup is automatically deleted.

Crashplan currently keeps infinite data and will overwrite only on instruction.

13. Retention and disposal of data

Daisy Chain discourages the keeping of personal, identifiable data for longer than is absolutely necessary. A considerable amount of data is collected on current trustees, staff, volunteers, students and families. However, once one of the above has ended their relationship with the organisation, it will not be necessary to retain all of the information held on them. Further information on the retention and disposal of personal data can be found in the Data Retention policy.

14. Disclosure of data

Daisy Chain must ensure that personal data is not disclosed to any unauthorised third parties. All trustees, staff and volunteers should exercise extreme caution when asked to disclose personal information held on another individual to a third party. For the avoidance of doubt, it is recommended that confirmation is sought from the DPO or a member of the Senior Leadership Team before releasing any information.

Personal data can be legitimately disclosed where one of the following criteria are met:

a. where the individual has given their consent;
b. where the disclosure of information is in the legitimate interests of Daisy Chain.

GDPR allows the disclosure of personal information is requested for one of the following exemptions:

a. national security;
b. defence;
c. public security;
d. the prevention investigation, detection or prosecution of criminal offences;
e. other important interests, in particular economic or financial interests, including tax matters, public health and security;
f. the protection of judicial independence and proceedings;
g. breaches of ethics in regulated professions;
h. monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
i. the protection of the individual, or the rights and freedoms of others; or
j. the enforcement of civil law matters.

14a. Disclosure Data for Recruitment Purposes

The Code of Practice published under section 122 of the Police Act 1997 advises that it is a requirement that all registered bodies must treat DBS applicants who have a criminal record fairly and not discriminate because of a conviction or other information revealed. See further information below for recent changes to the disclosure of criminal information on DBS certificates.

The Code also obliges registered bodies to have a written policy on the recruitment of ex- offenders; a copy of which can be given to DBS applicants at the outset of the recruitment process.

Overview

- As an organisation assessing applicants' suitability for positions which are included in the Rehabilitation of Offenders Act 1974 (Exceptions) Order using criminal record checks processed through the Disclosure and Barring Service (DBS), Daisy Chain complies fully with the Code of Practice and undertakes to treat all applicants for positions fairly. Daisy Chain undertakes not to discriminate unfairly against any subject of a criminal record check on the basis of a conviction or other information revealed.
- Daisy Chain can only ask an individual to provide details of convictions and cautions that Daisy Chain are legally entitled to know about. Where a DBS certificate at either standard or enhanced level can legally be requested (where the position is one that is included in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 as amended) and where appropriate Police Act Regulations (as amended), Daisy Chain can only ask an individual about convictions and cautions that are not protected.
- Daisy Chain is committed to the fair treatment of its staff, potential staff or users of its services, regardless of race, gender, religion, sexual orientation, responsibilities for dependants, age, physical/ mental disability or offending background.
- Daisy Chain has a written policy on the recruitment of ex-offenders, which is made available to all DBS applicants at the outset of the recruitment process.
- Daisy Chain actively promotes equality of opportunity for all with the right mix of talent, skills and potential and welcome applications from a wide range of candidates, including those with criminal records. Daisy Chain select all candidates for interview based on their skills, qualifications and experience.
- An application for a criminal record check is only submitted to DBS after a thorough risk assessment has indicated that one is both proportionate and relevant to the position concerned. For those positions where a criminal record check is identified as necessary, all application forms, job adverts and recruitment briefs will contain a statement that an application for a DBS certificate will be submitted in the event of the individual being offered the position.
- Daisy Chain ensures that all those in Daisy Chain who are involved in the recruitment process have been suitably trained to identify and assess the relevance and circumstances of offences. Daisy Chain also ensures that they have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, e.g. the Rehabilitation of Offenders Act 1974.
- At interview, or in a separate discussion, Daisy Chain ensures that an open and transparent conversation exists regarding any history that falls outside of a DBS check.

15. Safeguarding children, young people and adults

In the event that there is a safeguarding concern in relation to an individual accessing the services offered by Daisy Chain this matter should be passed to the designated safeguarding officer without delay – see the relevant Daisy Chain Safeguarding Policy.

The issue of safeguarding is a matter that is not specifically referenced within GDPR, however, it is supported by the Data Protection Act 2018. DPA allows organisations to process information if:

a) the processing is necessary for the purposes of:–

i) protecting an individual from neglect or physical, mental or emotional harm; or
ii) protecting the physical, mental or emotional well-being of an individual.

b) the individual is:–

i) aged under 18, or;
ii) aged 18 or over and at risk.

c) the processing of the information is carried out without the consent of the data subject for one of the following reasons:–

i) in the circumstances, consent to the processing cannot be given by the data subject;
ii) in the circumstances, Daisy Chain are unable to be reasonably expected to obtain the consent of the data subject to the processing;
iii) the processing must be carried out without the consent of the data subject as obtaining consent would prejudice the provision of the protection mentioned in section 15(a).

For the purposes of clarity, the DPA recognises an individual aged 18 or over is 'at risk' if there is reasonable cause to suspect that the individual:–

i) has needs for care and support;
ii) is experiencing, or at risk of, neglect or physical, mental or emotional harm; and
iii) as a result of those needs is unable to protect himself or herself against the neglect, harm or risk of it.

16. Profiling and marketing

Daisy Chain does not undertake any profiling on its service users or supporters nor is there currently any plans to do so.

For the purposes of marketing, Daisy Chain requires and asks for the permission of the individual. This is done on an 'opt in/opt out' basis, and at any time the individual has the option to opt in or opt out of marketing.

Daisy Chain issues regular newsletters to its service users and supporters. This is done using mailchimp. Under the terms and conditions of mailchimp, individuals must also provide their consent for their personal data to be used.

17. Archiving of data

Under GDPR, organisations are only permitted to store data for no longer than is necessary ('storage limitation'). The timescales for which data is kept is dependent on that nature of the information (for example, documents relating to

insurance policies [employers' liability/public liability] are to be kept indefinitely). Details relating to vehicular insurance may be disposed of if there has been no claims during the life of that policy.

If data is required for statistical purposes, all person identifiable information is to be removed ('pseudonymisation'). Additional information can be kept so long as it is separate and personal data cannot, and is not attributable to a natural person.

18. Use of CCTV

Daisy Chain uses CCTV for the purposes of preventing and detecting crime. Only staff authorised under the Daisy Chain CCTV policy and the organisations DPO can access the system. Recorded images will be kept for a timescale of no longer than 30 days. This can be less depending on activity.

Any requests for images from CCTV should be directed to either the Site Manager or DPO.

Footage that has been removed from the system will be destroyed as soon as any investigations have concluded.

Further information about Daisy Chain's use of CCTV is in the CCTV Policy.

19. Data Protection Impact Assessments

To ensure the correct use of personal data, each department will be required to complete a Data Protection Impact Assessment (DPIA). This will help to ensure that the adequate safeguards are in place to protect the personal data that is being processed by Daisy Chain.

New projects within Daisy Chain will be required to complete the DPIA in its entirety (see annex D). This will also form part of the processes of assigning a lawful basis for processing to each new area.

As projects evolve, the need for processing data will change, it is therefore important that the project lead and the DPO regularly review the data (initially 3 months after the start of a new project, then again if there are any amendments made to the data that is required) that is being processed. All DPIA's should then be reviewed annually.

20. Lawful basis for processing – new projects

It is important that before any new project that requires the processing of person identifiable information commences that a clear and appropriate lawful basis for processing has been assigned.

Once it has become clear that what data is to be recorded, the Information Commissioner's Office Lawful basis interactive guidance tool is to be used to assist in the decision process. This can be found at https://ico.org.uk/for-organisations/resources-and-support/lawful-basis-interactive-guidance-tool/

This information should then be passed to the DPO to review and document the assigned lawful basis for processing.

Annex A

Lawful basis for processing

- You must have a valid lawful basis in order to process personal data

- There are six available bases for processing. No single basis is 'better' or more important than another – which basis is most appropriate to use will depend on your purpose and relationship with the individual

    1) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose

    2) **Contract:** the processing of data is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering in to a contract

    3) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)

    4) **Vital interests:** the processing is necessary to protect someone's life

    5) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

    6) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Further information on lawful basis for processing can be found at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#ib3

Annex B

Explanation of key principles of GDPR

Article 5 of the GDPR sets out the following principles which are at the heart of the General Data Protection Regulation.

Article 5(1) requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals **('lawfulness, fairness and transparency')**;

b. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes; further processing for the purpose of archiving in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes **('purpose limitation')**;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that any personal data that is inaccurate, is rectified or erased without delay **('accuracy');**

e. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals **('storage limitation')**;

f. 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 **('integrity and confidentiality')**.

g. being responsible for compliance in line with GDPR, being proactive and organised about your approach to data protection, while demonstrating compliance mean that it must be possible to evidence compliance with the GDPR **('accountability')**.

Annex C

Definitions

a. **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular 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 natural person;

b. **'processing'** means 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 collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

c. **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

d. **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

e. **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

f. **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

g. **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

h. **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

i. **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

j. **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

k. **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

l. **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

j. **'special category data'** means any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health of data concerning a natural person's sex life of sexual orientation Definition taken from Article 9(1) of the General Data Protection Regulation).

k. **'function creep'** means the gradual widening of the use of a technology, system or data beyond the purpose for which it was originally intended, especially when it leads to a potential invasion of privacy.

Annex D

Data Protection Impact Assessment Template

Step 1: Identify the need for a DPIA

Explain what the project aims to achieve and what type of processing it involves. Other documents, such as proposals, can be link to this. Summarise why you have identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: How will you collect, use store and delete data? What is the source of the data? Will you be sharing it with anyone? What types of processing identified as likely high risk are involved?
Describe the scope of the processing: What is the nature of the data, and does it include any special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals will be affected? What geographical area does it cover?

Describe the context of the processing: What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children and vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in anyway? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with the relevant stakeholders: Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? * How will you ensure data quality and data minimisation? What information will you give individuals? How will you help support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

DAISY CHAIN DATA PROTECTION IMPACT ASSESSMENT (STEP 5)

Subject of Assessment	**Assessed By: -**
Person(s) at Risk:	

Severity of Harm	**Level**	**Likelihood of Occurrence**	**Level**
Severe	3	Probable	3
Significant	2	Possible	2
Minimal	1	Remote	1

Risk = Severity x Likelihood (Guidelines only): 1 - 3 Low 4 - 6 Medium 7 - 9 High

Project Name	**Hazards**	**Severity**	**Likelihood**	**Initial Risk Rating**	**Controls**	**Severity**	**Likelihood**	**Residual Risk Rating**	**Approved (Y/N)**

Signed	**Name:**	**Date:**
Counter signed:	**Name:**	**Date:**

Step 6: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		
Residual risks approved by		
DPO advice provided		
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, why?
Comments		
Consultation responses reviewed by:		If your decision departs from individuals' views you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA