GDPR Compliance. V1.0

Information security

Version	ISMSP207 / GDPR Compliance / v1.0
Author	Graeme Del-Nevo
Approval date	Aug 18
Date Issue	Aug18
How is policy to be disseminated	NETconsent

GDPR Privacy Notice

Who we are

We are a charitable trust providing treatment, support and accommodation to clients who are affected by, or are at the risk of being affected by substance misuse, and those involved in or at risk of becoming involved in the criminal justice system.

What is a privacy notice?

A Privacy Notice is a statement by the Trust to all stakeholders that describes how we collect, process, retain and disclose personal information which we hold. It is sometimes also referred to as a Privacy Statement, Fair Processing Statement or Privacy Policy. This privacy notice is part of our commitment to ensure that we process your personal information/data fairly and lawfully.

Why issue a privacy notice?

The Nelson Trust recognises the importance of protecting personal and confidential information in all that we do and takes care to meet its legal and regulatory duties. This notice is one of the ways in which we can demonstrate our commitment to our values of being transparent and open, and commitment to our values of Respecting Diversity, Acting with Integrity, Demonstrating Compassion, Striving for Excellence and to Listening and Supporting Others.

This document clearly expresses the policies of The Nelson Trusts management of personal information and is accessible to anyone upon request.

This notice also explains what rights you have to control how we use your information.

What are we governed by?

The key pieces of legislation/guidance we are governed by are:

Data Protection Act 1998
Human Rights Act 1998 (Article 8)
Access to Health Records Act 1990
Freedom of Information Act 2000
Health and Social Care Act 2012, 2015
Public Records Act 1958
Copyright Design and Patents Act 1988
The Re-Use of Public Sector Information Regulations 2015
The Environmental Information Regulations 2004
Computer Misuse Act 1990
The Common Law Duty of Confidentiality
The Care Record Guarantee for England
The Social Care Record Guarantee for England
International Organisation for Standardisation (ISO) – Information Security Management Standards (ISMS)
Information Security Management –
Records Management – Code of Practice for Health and Social Care 2016
Accessible Information Standards (AIS)
General Data Protection Regulations (GDPR) – post 25th May 2018

Who are we governed by?

Information Commissioner's Office - https://ico.org.uk/

Care Quality Commission - http://www.cqc.org.uk/

Why and how we collect information

We may ask for or hold personal confidential information about you which will be used to support delivery of appropriate care and treatment. This is to support and help meet our purpose of ensuring the provision of safe, effective and compassionate high quality care.

Data is lawfully processed using legitimate interests and consent obtained under article 6 1(f) and 1(a) and special category data obtained under article 9.2(d), stored and processed solely to assist staff and volunteers in the efficient running and monitoring of the service and service improvement. Personal details supplied by all stakeholders are only used to send material that is considered potentially useful. This data is stored securely on the Nelson Trust database with access restricted to appropriate identified personnel.
The trust commits to only processing necessary data that is targeted and proportionate to achieve its lawful and legitimate purpose of providing services that benefit society. Accordingly the trust employs technical, contractual and administrative steps to ensure information is protected against unauthorised access and disclosure. Nelson Trust employees undertake training in handling information with particular emphasis on preserving the privacy and interests of individuals.

Information collected may include:

- Basic details, such as name, address, date of birth, next of kin.
- Contact we have had, such as appointments and home visits.
- Details and records of treatment and care, including notes and reports about your health
- Information from people who care for you and know you well, such as health professionals and relatives.
- Criminal offences and convictions

It may also include personal sensitive information such as sexuality, race, your religion or beliefs, and whether you have a disability, allergies or health conditions. It is important for us to have a complete picture, as this information assists staff involved in your care to deliver and provide improved care, deliver appropriate treatment and care plans tailored to meet individual's needs.

Information is collected in a number of ways, via Recovery/Keyworkers workers, HR staff, Admissions and fundraising teams and other Nelson Trust staff.

How we use information

To help inform decisions that we make about service users care.
To ensure that treatment is safe and effective.
To work effectively with other organisations who may be involved in individuals care.
To support the health of the general public.
To ensure our services can meet future needs.
To review care provided to ensure it is of the highest standard possible.
To train our staff.
For audit.
To prepare statistics on Nelson Trust performance.

To monitor how we spend public money.

There is huge potential to use information to deliver care and improve health and care services across the Nelson Trust. The information can be used to help:

- Improve individual care.
- Develop new treatments and prevent addiction.
- Plan services.
- Improve client safety.
- Evaluate Government Contacts.

It helps you because;

- Accurate and up-to-date information assists us in providing the best possible care for our service users.
- All appropriately identified staff members can readily access the information they need to provide the best possible care.
- Where possible, when using information to inform future services and provision, non-identifiable information will be used.

The Nelson Trust will not use personal information about an individual for the purposes of direct marketing.

Information about or own staff and people applying to work for or with us

We need to process personal data about our own staff (and people applying to work for us) so that we can carry out our role (for example, by ensuring that we have the right staff to support individuals accessing services) and so we can meet our legal and contractual responsibilities as an employer.

The personal data that we process includes information about racial or ethnic origin, religion, disability, gender and sexuality. We use this information to check we are promoting and ensuring diversity in our workforce and to make sure we are complying with equalities legislation.

Our employees decide whether or not to share this monitoring data with us, and can choose to withdraw their consent for this at any time. Employees who wish to withdraw their consent for us to process this data can contact the HR team.

If you apply for a job with us, we will have a legitimate interest to process the personal data supplied. Processing this data is necessary in order to ensure a proper application process.

Your personal data will be retained for 6 months after the vacancy has been filled.

We share information about our employees as required to meet our contractual obligations to them – for example, by sharing relevant information with our payroll bureau and pension service administrators.

Other personal data that we are required to process includes information on qualifications and experience, pay and performance, contact details, bank details, and service records (including records of continuous service and pension contributions/entitlements).

We check that people who work for us are fit and suitable for their roles. This may include asking people to undertake Disclosure and Barring Service (DBS) checks.

How information is retained and kept safe?

Information is retained in secure electronic and paper records in accordance with the requirements of GDPR and access is restricted to only those who need to know.

It is important that information is kept safe and secure, to protect your confidentiality. There are a number of ways in which your privacy is shielded; by removing your identifying information, using an independent review process, adhering to strict contractual conditions and ensuring strict sharing or processing agreements are in place.

In order to demonstrably guarantee the security of your personal data The Nelson Trust has an ISO 27001 certification.

GDPR regulates the processing of personal information. Strict principles govern our use of information and our duty to ensure it is kept safe and secure.

The Nelson Trust is registered with the Information Commissioners Office (ICO). Details of our registration can be found on

https://ico.org.uk/esdwebpages/search enter our registration number (Z9720653) and click 'search register' Z9720653

Technology allows us to protect information in a number of ways, in the main by restricting access. Our guiding principle is that we are holding your information in strict confidence.

We have a retention and disposal schedule which explains how long we keep different types of records and documents for, including records and documents containing personal data. Personal data is deleted or securely destroyed at the end of its retention period.

How do we keep information confidential?

Everyone working for the Trust is subject to the Common Law Duty of Confidentiality and GDPR. Information provided in confidence will only be used for the purposes necessary for which it has been collected, unless there are other circumstances covered by the law.

Under the Nelson Trust Confidentiality Code of Conduct, all staff are required to protect information, inform you of how your information will be used and allow you to decide if and how your information can be shared. This will be noted in your records.

All Trust staff are required to undertake annual training in GDPR, data protection, confidentiality, ISMS Policy, with additional specialist training for specific staff members, such as data protection officers and IT staff.

Volunteer placements take place within the Nelson Trust. This may be when you are in one of our treatment houses or in a community setting such the Woman's Community Centers.

If staff would like a volunteer to be present, they will always ask for your permission prior to any meeting takes place. The treatment or care you receive will not be affected if you refuse to have a volunteer present during your period of care.

Occasionally, for assessment purposes, volunteers may request that their supervisor be present. You may refuse this if it makes you feel uncomfortable.

Who will the information be shared with?

- To provide best care possible, sometimes we will need to share information about you with others. We may share your information with a range regulatory bodies. You may be contacted by any one of these organisations for a specific reason; they will have a duty to tell you why they have contacted you. Information sharing is governed by specific rules and law.
- When the health or safety of others is at risk or where the law requires the disclosure of information.
- We may also be asked to share basic information about you, such as your name and parts of your address, which does not include sensitive information from your records. Generally, we would only do this to assist them to carry out their statutory duties. In these circumstances, where it is not practical to obtain your explicit consent, we are informing you through this notice, which is referred to as a Privacy Notice, under the GDPR
- Where client information is shared with other organisations, an information sharing agreement is drawn up to ensure information is shared in a way that complies with relevant legislation.
- Other organisations we share information with may include, but are not restricted to: social services, education services, local authorities, the probation service, the police, voluntary sector providers and private sector providers.
- You have the right to refuse/withdraw consent to information sharing at any time. We will fully explain the possible consequences to you, which could include delays in you receiving treatment and care.

We use a third-party supplier to print our invitations to events and other literature. If you subscribe to this service, your name and email address will be shared with them.

The third-party supplier handles the data purely to provide this service on our behalf. This supplier observes the requirements of the Data Protection Act 1998 in how they obtain, handle and process your information. They will not make your data available to anyone other than The Nelson Trust without your permission.

Your Rights

Access to your personal data. You may ask us whether we process personal data of you. If that is the case we will explain what personal data about you is processed by us, in what way and for what purposes we do this. You may also request from us a copy of your personal data that we process;

Rectification of your personal data. In case it is your opinion that your personal data that we process, is incorrect or incomplete, you can make a request for to have inaccurate data rectified, or completed if it is incomplete.

Erasure of your personal data. You may request erasure of your personal data that we process. After receipt of a request to that effect we will erase your personal data without undue delay if:

- The data is no longer necessary for the purpose for which it has been processed by us;
- You do not give us your consent to process your personal data any longer;
- You object to the processing of the personal data and there is no reason why we may process the data any longer;
- The personal data should not have been processed by us ('unlawful processing');
- The law requires us to erase the personal data.

Restriction of processing of your personal data. In some cases you may wish that the processing of your personal data is restricted. In that case you may request from us restriction of processing. We will comply with such a request in the following cases:

- It is your opinion that your personal data which we process, is incorrect. We will not use this personal data until the data has been verified and possibly modified or completed;
- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) but you are opposed to erasure and request restriction instead
- We do not need your personal data any longer but you wish to be able to use this data in order to establish a claim or instigate legal proceedings;
- You object to our processing of your personal data and we have not yet evaluated your objection. If processing of your personal data is subject to a restriction, we will process this data only with your consent. Before the restriction is lifted, we will inform you of that.

Right to data portability. In some circumstances you may request from us a copy of your personal data which we process. We will provide you with a copy in a commonly used format which can be used for instance, if you wish to transfer the data to a different service provider, in the case where this is technically possible for us and if you wish, we can directly transmit the personal data to your new service provider.

You also have the right to **object** in writing to the processing of your personal data. In the case you do object, you must provide the grounds relating to your particular situation to why you do not agree with processing of your personal data.

Contacting us about your information

Each organisation has a senior person responsible for protecting the confidentiality of your information and enabling appropriate sharing.

If you have any questions or concerns regarding the information we hold on you, the use of your information or would like to discuss further, please contact the Data Controllers Graeme Del Nevo or Mark Wilson.

Data Controller
Nelson Trust
Port Lane
Brimscombe
Stroud
GL5 2QP
Phone: 0453 885633

Can I access my information?

Under GDPR a person may request access to information (with some exemptions) that is held about them by an organisation. For more information on how to access the information we hold about you please refer to https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Contacting us if you have a complaint or concern

We try to meet the highest standards when collecting, processing, storing and using personal information. We encourage people to bring concerns to our attention and we take any complaints we receive very seriously. You can submit a complaint through the Trust's Complaints Procedure, or you can write to:

Data Controller
Nelson Trust
Port Lane
Brimscombe
Stroud
GL5 2QP
Phone: 01453 885633

If you remain dissatisfied with the Trust's decision following your complaint, you may wish to contact:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Their web site is at www.ico.gov.uk The Information Commissioner will not normally consider an appeal until you have exhausted your rights of redress and complaint to the Trust.

If you need further clarification, please contact Graeme Del-Nevo 01453 885633

Subject Access Request Procedure

Scope

The Data Protection Act 1998 (DPA) and GDPR provides individuals with rights in connection with personal data held about them. It provides those individuals with a right of access to that data subject to the rights of third parties and the satisfaction of a number of criteria as outlined in the Data Protection Policy (see ISMSP36). This procedure defines the process to be followed when a request for access to personal data is received. A subsequent failure to comply with the provisions of the DPA and GDPR in responding to this request may render the Nelson Trust, or in certain circumstances the individuals involved, liable to prosecution as well as giving rise to civil liabilities.

Responsibilities and Definitions

Records and Information Manager is the Nelson Trust Data Protection Officer and is responsible for ensuring that statutory and regulatory obligations with respect to the DPA and GDPR are adhered to.

Data Controller is responsible for handling subject access requests.

Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information.

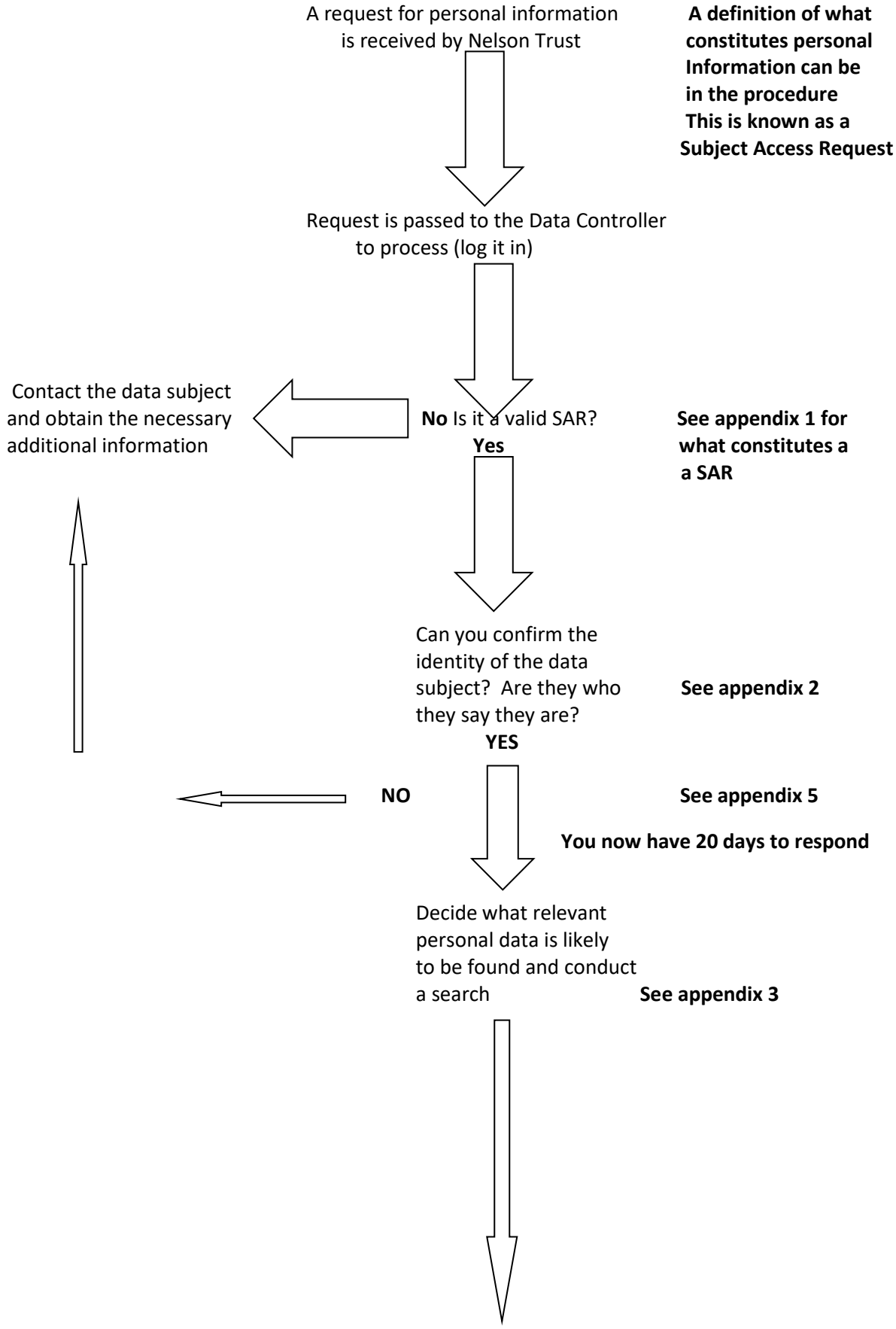
Data Controller is the person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be, processed. In our case the Graeme Del Novo is the registered Data Controller.

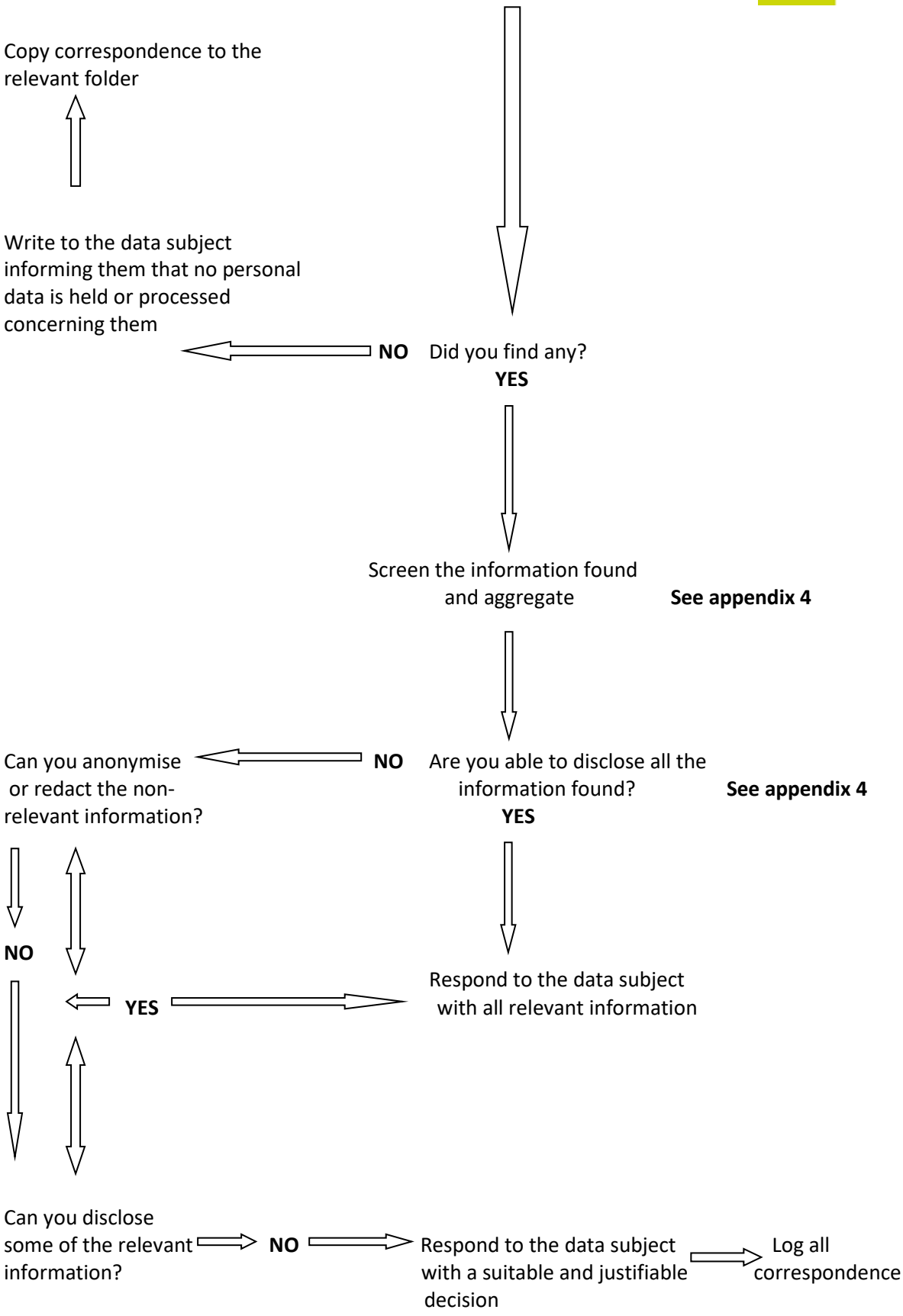
Data Processors are any individual or company who records and/or processes personal data in any form in compliance of the Non-Disclosure Agreement and therefore subject to the requirements of this policy. Compliance with this policy is normally managed by contract.

Nelson Trust permanent and temporary employees, contractors and consultants are responsible for incorporating this procedure and its associated policy into their own working practices.

The definitions of the terms used in this procedure are as defined in the Nelson Trust's Data Protection Policy which should be read in conjunction with this procedure.

Procedure


A request for personal information is received by Nelson Trust
A definition of what constitutes personal Information can be in the procedure This is known as a Subject Access Request
Request is passed to the Data Controller to process (log it in)
Contact the data subject and obtain the necessary additional information
No Is it a valid SAR?
Yes
See appendix 1 for what constitutes a a SAR
Can you confirm the identity of the data subject? Are they who they say they are?
See appendix 2
YES
NO
See appendix 5
You now have 20 days to respond
Decide what relevant personal data is likely to be found and conduct a search
See appendix 3


Copy correspondence to the relevant folder
Write to the data subject informing them that no personal data is held or processed concerning them
NO
Did you find any?
YES
Screen the information found and aggregate
See appendix 4
Can you anonymise or redact the non-relevant information?
NO
Are you able to disclose all the information found?
See appendix 4
YES
NO
YES
Respond to the data subject with all relevant information
Can you disclose some of the relevant information?
NO
Respond to the data subject with a suitable and justifiable decision
Log all correspondence

Documentation

• Records of communications relating to a subject access request (Retained for 5 years)
• Records of communications resulting in an action to cease processing personal data (Retained for 5 years)

Appendices

Appendix 1: What does a valid SAR look like?

A valid subject access request is one which the Data Controller decides;

Provides all the information they require to locate the information the person wants;

Provides sufficient information to verify the data subject's identity.

It is unlikely that the first contact from the data subject will provide all the relevant information and in which case the Data Controller must write to the data subject requesting this.

Once the data controller has received all the information they need and sufficient information to verify the data subject's identity, they have one month to provide the information requested.

Appendix 2: How to correctly identify a Data Subject.

Before disclosing any personal information the Data controller must verify the identity of the data subject.

Whilst it is important that Nelson Trust does not send copies of personal information to people who are not the data subject, they must not appear obstructive. The DPA and GDPR requires Nelson Trust to take "reasonable measures" to verify the identity of a data subject. The data controller should keep a record of what measures they take. If the evidence is insufficient and requires further verification of the data subject's identity, there are 2 options;

1. Telephone the individual and based on the information held about them ask two questions so as to confirm their identity.

2. Write to the individual and ask them to send the data controller a photocopy of their passport or driving licence (this option will take longer and it is also possible that the individual does not have a passport or drivers licence).

Appendix 3: Where to look for personal information.

Based on their knowledge of the business area, the Data Controller should decide where 'personal data' about the individual concerned might be held, and locate that information. They may need to search central filing systems electronic and manual, personnel records, shared drives, the Intranet and/or private filing systems of particular individuals. If necessary, they must also ask colleagues to search their personal drives and e-mail accounts.

If staff are aware of other business areas that might also hold information about the person concerned, please tell the Data Controller as soon as possible so that they can arrange for these areas to be searched.

Staff do not have to look through unstructured personal data unless a specific piece of information has been requested and its location identified. However they do have to look through any semi-structured data and for information held in a relevant filing system (see the definitions above).

If the cost of supplying the data is likely to be excessive advise the Data Controller as Nelson Trust may charge a fee in line with the Freedom of Information and Data Protection Regulations 2004.

Appendix 4: How to screen information & what can and cannot be disclosed as a result of a SAR

Once the Data Controller has collected together the information we hold about a data subject they must examine it in detail to establish if it should be disclosed. This must be done on a case-by-case basis for each individual piece of information. In some cases they might have to disclose only parts of particular documents.

1. Check that the record is actually about the person concerned and not about someone else with the same name. Just because a record contains somebody's names does not always mean that it is about them. For example, an e-mail might carry the subject line "Meeting about John Smith" but if the e-mail only contains details about whether people can attend the meeting the e-mail is not about John Smith. The Data Controller should only print out records/documents/e-mails which are about the person making the subject access request.

2. Screen out any duplicate records. For example if there has been an e-mail exchange with some colleagues, the Data Controller only needs to print out the last e-mail in the exchange if copies of all the other e-mails are part of the last e-mail.

3. If a record was created by a member of staff acting in a private rather than an official capacity, only exceptional circumstances would justify its disclosure without their consent. If they are not prepared to disclose the record, do not disclose it. Please note however that the Nelson Trust's IT policies do not permit personal use of the computing facilities.

4. The Data Controller should only disclose information which is about the person making the subject access request. Where a document contains personal data about a number of individuals, including the data subject, they should not disclose the information about the third parties to the data subject. If the record is primarily about the data subject, with incidental information about others, they should redact the third party information. If the record is primarily about third parties withhold it if redacting is not possible. Alternatively, contact the third party to obtain consent to disclose the document if possible.

5. The records may contain correspondence and comments about the data subject from a number of parties, including private individuals, external individuals acting in an official capacity, and Nelson Trust staff. In these cases we are required to balance the interests of the third party against the interests of the data subject and often omit or redact third party information.

6. Do not disclose information which would prejudice the prevention or detection of a crime. For example, if the Police informed us that a member of staff is under investigation, but the member of staff did not know this, then we should not provide that information to the member of staff whilst

the investigation is in progress. However, if the investigation is closed or if the member of staff has been informed that there is an investigation underway, then the information should be disclosed in response to a subject access request.

7. We should not disclose any records which contain advice from our lawyers, where we are asking for legal advice or which were written as part of obtaining legal advice.

8. Do not disclose information which is being used, or may be used in future, in negotiations with the data subject if the information gives away our negotiating position and disclosing the information would weaken that negotiating position.

The exemptions identified above are those most likely to apply to information held by the Nelson Trust. There are others and it is good working practice to research all DPA and GDPR exemptions before responding to a SAR.

As the Data Controller puts the information together they may discover material which does not reflect favourably on us. For example, they may find documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject. These documents must be disclosed. However, the Data Controller should bring their contents to the attention of the relevant manager and ensure that appropriate action is taken to address any issues they raise.

Staff must not destroy or refuse to disclose records because they would be embarrassing to disclose. This is a criminal offence if it is done after you know a subject access request has been made.

Once the Data Controller has identified all of the information that can be sent in response to a SAR, one final review of this information as a collection must be made. This is to offset the risks often discovered by aggregating information. For example, the Data Controller may have identified that all the information they intend to release is unrestricted in its nature. However, once aggregated there is an inherent risk that additional information could be disclosed or at least interpreted. This has to be taken into consideration before the final response is made.

Appendix 5: How to log the requests and responses.

The Data Controller should **Create a folder for each SAR** – the filename should be made up from the reference number and surname of the applicant e.g. SAR2011010 – Smith.
For each SAR file the following;

Copies of the correspondence between the Data Controller and the data subject and between the Data Controller and any other parties.
A record of any telephone conversation used to verify the identity of the data subject.
A record of the Data Controller's decisions and how they came to those decisions.
Copies of the information sent to the data subject, for example if the information was anonymised keep a copy of the anonymised or redacted version that was sent.

The folder should be kept for 5 years and then securely destroyed within the Nelson Trust's records management programme.

Appendix 6: DATA PROTECTION ACT 1998 and GDPR: Subject Access Request Template

I understand that you wish to exercise your rights under the Data Protection Act 1998 (“the DPA") and GDPR to;

• be given a description of any personal data which we may hold on you;
• be advised of the purposes for which this data may be used;
• be notified of the identity of any person or organisation to whom the data may be disclosed; and
• be advised as to the source of the data.

[Delete one of the following two paragraphs as appropriate]

The Nelson Trust are obliged under the DPA and GDPR to satisfy ourselves as to the identity of the person making the request and accordingly we require you to complete the attached Subject Access Request Form, countersigned by your HR Manager or line manager to confirm your identity. In the case of contractors, the nominated Nelson Trust representative for your project should confirm your identity. We regret that we will be unable to respond to your request without this information.

The Nelson Trust are obliged under the DPA and GDPR to satisfy ourselves as to the identity of the person making the request. Accordingly, we require you to complete the attached Subject Access Request Form and provide suitable proof of your identity such as your original passport or a copy certified by a solicitor of your original passport, plus original utility bills from at least two service providers to your home address.

Also, in order to assist the Nelson Trust to locate the information which you are seeking in a timely and efficient manner, you should provide as much information as possible as to the type of data which you are seeking, the period during which the data has been held, the persons or departments who are likely to be holding this data and the sites and/or specific locations where such persons or departments are based.

Please send the completed form and any necessary evidence (as appropriate) to The Data Controller, The Nelson Trust, Port Lane Brimscombe Stroud Glos GL5 2QJ.

We will endeavour to respond to your request as soon as reasonably practicable.

Employee Subject Access Request form

I am/was an employee of the Nelson Trust and wish to exercise my rights under the Data Protection Act 1998 and GDPR to:

- be given a description of the personal data which you may hold on me;
- be advised of the purposes for which this data may be used;
- be notified of the identity of any person or organisation to whom the data may be disclosed; and
- be advised as to the source of the data.

To assist you to locate the data, the information which I require can be categorised as follows:-

Type or Class of Information	Period Data Held	Nelson Trust Department(s) Holding the Information	Location of Department(s)

Please continue on another sheet if necessary

I can be contacted on ……..and my home address is ……
……

I certify that_____ [Name] _____ [Employee No] is an employee/Ex-employee [

Transferring Data from the EU Procedures Privacy Shield and Data Transfer under the GDPR

In line with EU Data Protection Directive 1995, Nelson Trust will ensure that any of its data transferred to non-EU countries will receive an adequate level of protection upon arrival in the destination country.

Nelson Trust will transfer its personal data to the US if necessary under the provisions of the EU Data Protection Directive 1995 under the following mechanisms that will allow such transfers which will include:

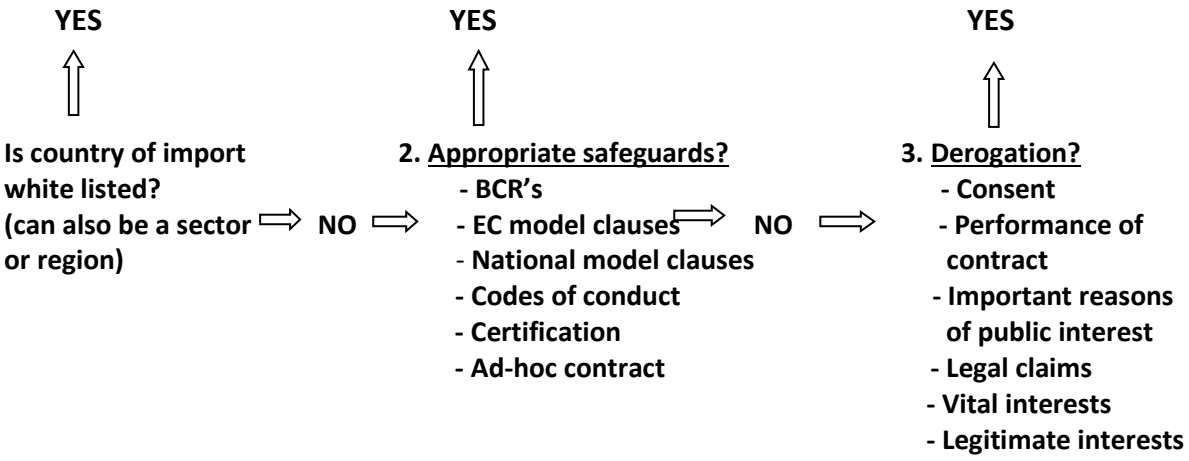
- An "adequacy decision" by the European Commission
- EU-sanctioned "appropriate safeguards" for transfers such as model clauses
- Statutory exceptions to the general transfer prohibition, such as consent or contractual obligations

In addition to this, Nelson Trust will adopt the GDPR new transfer mechanisms such as:

- Certifications and
- Approved codes of conduct

In the absence of appropriate safeguards, Nelson Trust will use the GDPR's clear "last choice" for transfer mechanisms which is an enumerated list of derogations permitting limited data transfers to non-EU countries.

Graphically represented, the GDPR's transfer –mechanism hierarchy in use at Nelson Trust will appear as follows:



Pseudonymisation and Anonymisation of Data Policy

Introduction

A fundamental principle of the Data Protection Act 1998 and GDPR is to use the minimum personal data to satisfy a purpose and to strip out information relating to a data subject that is not necessary for the particular processing being undertaken. This principle is aligned with the Caldicott Principles familiar to NHS and Social Care organisations and is supported by both common law confidentiality obligations and the Human Rights Act 1998 which provides a privacy right for individuals.

There is also a requirement that organisations respect people's private lives unless there is a lawful exemption to the Human Rights requirements and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

The key principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that are used to support purposes other than their direct care or to quality assure the care provided. Where this is not practicable data should flow through business processes that minimise the risk to data. In many circumstances this requires data to be received by a part of the organisation designated as a 'safe haven' where it can be processed securely and only used in an identifiable form for specific authorised procedures within the safe haven boundary. Onward disclosure should be limited to pseudonymised or anonymised data.

Effective pseudonymisation and/or anonymisation processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality.

Scope

This policy is specifically concerned with the security of client level clinical data when used for purposes other than direct client care including, but not limited to:

- Staff Pensions
- Injury Benefit
- HR Records;
- Client Records

This policy is in line with our Operating Framework.

Purpose

This document seeks to provide all Nelson Trust's personnel who use client level clinical data with guidance to safeguard the confidentiality when the data is used for purposes other than direct client healthcare.

Definitions

- Personal Identifiable Data (PID) – is any information that can identify one person. This could be one piece of data for example a person's name or a collection of information for example name, address and date of birth.

- Primary Uses – is when information is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

- Secondary Uses – is for non-healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When PID is used for secondary use this should, where appropriate, be limited and de-identified so that the secondary uses process is confidential.

Responsibilities

Ultimately responsibility for this Policy rests with the Nelson Trust Leadership Team, but on a day-to-day basis the Information Governance and GDPR steering committee and the Data Controller will be responsible for managing and implementing the Policy.

The Data Controller is responsible for ensuring that the designated training in areas of Data Protection and Information Security cover Anonymisation and Pseudonymisation.

All staff are responsible for compliance with the policies and procedures as well as identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising Data Controller accordingly.

Business Processes

All business processes using client level personal data, within the Nelson Trust must be documented.

Business processes can include, but are not limited to:

- The process for using personal data for secondary uses;

- The use of PID for a combination of primary and secondary.

Primary use includes, but is not restricted to the client treatment details or inputting test results. All information recorded about a person should be recorded in line with the Nelson Trust's Records Management Policies, the Data Protection Act 1998 and GDPR.

Secondary use business processes should be initially documented and then reviewed regularly to assess any requirement to use de-identified data. Following assessment any processes that require de-identified data must be modified in line with this policy.

All onward disclosure should be limited to pseudonymised or anonymised/de-identified data.

Anonymisation / De-identification

Staff only have access to the data that is necessary for the completion of the business activity which they are involved in. This is reflected in Caldicott Principles; access should be on a need to know basis. This principle applies to the use of PID for secondary or non-direct care purposes. By de-identification users are able to make use of client level clinical data for a range of secondary purposes without having to access the identifiable data items.

The aim of de-identification is to obscure the identifiable data items within the persons records sufficiently that the risk of potential identification of the subject or a person's record is minimised to acceptable levels, this will provide effective anonymisation. Although the risk of identification cannot be fully removed this can be minimised with the use of multiple pseudonyms.

De-identified data should still be used within a secure environment with staff access on a need to know basis.

De-identification can be achieved by:

- Removing direct patient identifiers;
- The use of identifier ranges, for example; value ranges instead of age;
- By using a pseudonym.

If client data is required the Nelson Trust client registration number is the most secure form of identifiable data. The Nelson Trust registration number should be included within all client records and documentation in line with the current Connecting for Health NHS Number Campaign.

Pseudonymisation

When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual clients across different data sets and over time. This allows the linking of data sets and other information which is not available if the PID is removed completely.

To effectively pseudonymise data the following actions must be taken:

- Each identifying field of PID must have a unique pseudonym;
- Pseudonyms to be used in place of Nelson Trust registration numbers and other fields must be of the same length and formatted on output to ensure readability. For example, in order to replace Nelson Trust's registration numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an Nelson Trust registration number to avoid confusion with original Nelson Trust registration numbers;

- Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports;
- Where used pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised;
- The secondary use output must, where pseudonyms used, only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines;
- Pseudonymised data should have the same security as PID.

Use of identifiable data

If client records are viewed in an identifiable form then the reasons and usage of the data should be fully documented and approval is required by the appropriate data owner. This auditable trail of access to client's records supports the Care Record Guarantee where patients are to be informed as to who has accessed/seen their data and the audit will provide accurate data in the event of untoward incidents.

The key items to be documented are:

- Who has accessed each data base containing identifiable data;
- Date and time of access;
- The reason for the access;
- The output from the access.

This audit should be kept within a separate structured database to enable queries and audit.

The log of accesses must be regularly audited via sampling of users or subject matter to check for unusual patterns of access. If any unusual patterns of access are noted this should be reported via the Data Controller.

Transferring Information

Appropriate data sharing agreements should be in place when information is to be transferred to another organisation. If the transfer of information is required for secondary use then a form of anonymised or pseudonymised data should be sent.

Legal and professional obligations

All Nelson Trust's client records are Public Records under the Public Records Act. The Data Controller will take actions to comply with the relevant legal and professional obligations, in particular:

- The Caldicott Principles;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Common Law Duty of Confidentiality;
- Nelson Trust Information Security Operating Framework; and
- The Nelson Trust's Confidentiality Code of Practice.

Training

All Nelson Trust staff will be made aware of their responsibilities relating to this policy through generic and specific training programmes and guidance.

Validity of this Policy

This Policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

This Policy should be reviewed annually under the authority of the Data Controller. Anonymisation and pseudonymisation standards should be subject to an ongoing development and review programme.

References

- NHS Connecting for Health IG Toolkit
- NHS Operating Framework 2011/12
- Caldicott Committee Report 2012

EU Model Clauses

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the **data exporting** organisation: _____

Address:

_____

_____

_____

Tel.: ..... Fax: .....

E-mail: .....

Other information needed to identify the organisation

……
(The **data exporter**)

And

Name of the **data importing** organisation: Nelson Trust

Address:

_____

_____

_____

Other information needed to identify the organisation:

……

(**the data importer**)

each a "**party**"; together "**the parties**".

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1. 1

Definitions

For the purposes of the Clauses:

- 'Personal data' , 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- 'The data exporter' means the controller who transfers the personal data.

- 'The data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC.

- 'The subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- 'The applicable data protection law' means the legislation protecting the fundamental rights and
freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established.

- 'Technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the

transmission of data over a network, and against all other unlawful forms of processing.

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third- party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Obligations of the data exporter

The data exporter agrees and warrants:

- That the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State.

- That it has instructed and throughout the duration of the personal data processing services

will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses.

- That the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract.

- That after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- That it will ensure compliance with the security measures;

- That, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC.

- To forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

- To make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

- That, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and that it will ensure compliance with Clause 4(a) to (i).

Obligations of the data importer

The data importer agrees and warrants:

- To process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

- That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled

to suspend the transfer of data and/or terminate the contract.

- That it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred.

- That it will promptly notify the data exporter about:

    1. Any legally binding request for disclosure of the personal data by a law.
    2. Enforcement authority unless otherwise prohibited, such as a prohibition under.
    3. Criminal law to preserve the confidentiality of a law enforcement investigation.
    4. Any accidental or unauthorised access
    5. Any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so.

- To deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

- At the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority.

- To make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter.

- That, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent.

- That the processing services by the subprocessor will be carried out in accordance with Clause 11.

- To send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive

compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Mediation and Jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- To refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

- To refer the dispute to the courts in the Member State in which the data exporter is established.

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Cooperation with supervisory authorities

The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any

subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Variation of the Contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Obligation after the Termination of Personal Data Processing Services

The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the

data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address:

_____

_____

_____

Other information necessary in order for the contract to be binding (if any):

Signature……..

(Stamp of Organisation)

On Behalf of the Data Importer

Name (written out in full):_____

Position: _____

Address:

_____

_____

_____

Other information necessary in order for the contract to be binding (if any):

Signature…….

(Stamp of Organisation)

Data Processors Questionnaire

1. The current data protection legislation – the Data Protection (Bailiwick of Guernsey) Law, 2001 and the Data Protection (Jersey) Law 2005 (the Current Laws) – was drafted in response to EU Directive 95/46/EC (the Directive) and declared adequate for the purposes of data transfers. Given the vast changes in technology that have taken place over the last twenty years, the Current Laws (and European laws) are being updated.

2. The EU has approved the General Data Protection Regulation (GDPR), the largest change to the protection of personal data since the Directive in 1995. The GDPR comes into effect for EU Member States on 25 May 2018. Whilst the Channel Islands (the Islands) are not part of the EU, the GDPR has implications for the Islands in two ways:

    - Local organisations offering goods/services to or otherwise targeting/monitoring EU citizens will be required to comply with the GDPR, regardless of what regulatory or legislative regime is in place locally.
    - The Islands' "adequacy" rulings under the current EU Directive will be re-assessed against the GDPR and it is highly unlikely that the Current Laws will be considered adequate against the new standard. Both Governments have therefore made the decision that new legislation will be implemented in both Islands with the aim to be ready for implementation in May 2018, in line with the EU legislative timetable.

What do you need to do?

1. Legislative drafting across the Channel Islands is underway with a view to the creation of new, GDPRfocused data protection laws ("new data protection legislation") in both Bailiwicks. However, it may be some time before any drafts are available for review. That being so, it is important for organisations to take stock of their current data handling processes and procedures now and not to leave preparations until the last minute.

2. Whilst aspects of the GDPR are new, many of the requirements build upon the existing legislative framework and therefore compliance with the Current Laws will go a long way towards compliance with the GDPR. If your organisation is compliant under the Current Laws then much of your approach should remain valid under the GDPR. The GDPR does, however, introduce certain new elements and other significant enhancements and it is important and useful for organisations to identify and understand how the GDPR is likely to impact them. The responsibility to become familiar with the GDPR (and any local legislation in due course) lies with the organisation.

3. In addition to existing, published guidance the Commissioners has launched a microsite dedicated to GDPR and data protection reform. This can be found at www.thinkgdpr.org.

4. Further information will be provided over the coming months in order to assist in preparation for the GDPR (and the new legislation).

5. Do not underestimate the time required to ensure you are fully prepared for 2018. The value of formulating, adopting and implementing exemplary data governance and security practices lies in the rewards it yields.

Using this Questionnaire

1. In order to provide a practical starting point for organisations, the Commissioner has compiled the this questionnaire to assist in the preparation for compliance under the GDPR and new local legislation. This questionnaire contains simple questions that senior management and directors of organisations can use to assess the basic level of compliance that currently exists within that organisation and to highlight those areas which are likely to require attention prior to May 2018. It is also a starting point for the record of processing activities that data processors will be required to hold under both the GDPR (article 28) and local legislation. It is for your internal use only.

2. The document is protected so you will only be able to add, edit and delete text in the space given for answers.

3. Additional information to support some of the questions in this document can be found in the Data Processors' Self-Assessment Notes.

THIS DOCUMENT IS PURELY FOR GUIDANCE AND DOES NOT CONSTITUTE LEGAL ADVICE OR LEGAL ANALYSIS. IT IS INTENDED AS A STARTING POINT ONLY, AND ORGANISATIONS MAY NEED TO SEEK INDEPENDENT LEGAL ADVICE WHEN REVIEWING, ENHANCING OR DEVELOPING THEIR OWN PROCESSES AND PROCEDURES OR FOR SPECIFIC LEGAL ISSUES AND/OR QUESTIONS.