SAFE | WELL | PROSPEROUS | CONNECTED

Humber Information Sharing Charter

IG Doc Ref – DOC NLC06	Next Review Date – June 2020	Version v9.0
This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website. Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.		

This Charter supersedes all previous versions of this Charter including the Community Charter for Information Sharing (North East and North Lincolnshire) and the General Protocol for Information Sharing between agencies in Kingston upon Hull and the East Riding of Yorkshire.

North Lincolnshire Council

Contents

Humber Information Sharing Charter

Humber Information Sharing Charter

1. Introduction

1.1 The appropriate exchange of information is essential to deliver effective and efficient services for the public, to meet their needs and ensure their welfare and protection. However there is a balance between the need to share sufficient information to deliver effective services, and preserving the privacy of the individual.

1.2 To assist understanding and the application of effective information sharing it is important to have locally documented clarity about how legal constraints 'fit' with practice guidelines, identifying what can and cannot be shared with whom, when, how and for what purposes.

1.3 This Charter provides a two-tier framework for the effective and secure sharing of information in accordance with legal requirements, ethical boundaries and good practice across the Humber region. It will ensure transparency of information governance practices, assist the documenting of information sharing decisions and actions to ensure they are auditable, and raise awareness of the legal and ethical boundaries around information disclosure and the rules and methods for accessing data.

1.4 Tier 1 (The Charter) sets out the principles and standards under which the sharing of personal and non-personal information will take place.

1.5 Tier 2 (The Agreement) identifies the personal and non-personal information being shared and the operational arrangements in place for the secure sharing of information for a specific fair and lawful purpose.

1.6 Whilst there will only be one Tier 1 Charter, there will be many Tier 2 Information Sharing Agreements (Part A) with potentially multiple Data Set Lists (Part B) sitting underneath each of them.

1.7 The Charter does not impose new obligations on signatory organisations, but reflects current statutory, regulatory and legal obligations for the sharing of personal information, and builds on existing partnerships.

2. Objectives of the Charter

2.1 The signatories to this Charter recognise the importance of sharing information effectively and securely for the purposes of delivering and improving outcomes for individuals and the communities we serve.

2.2 This Charter aims to achieve consistent and good practice for the sharing of personal, sensitive and confidential information, by providing clear standards for the secure and confidential sharing of personal information in accordance with legal requirements.

3 Our commitment

3.1 As a signatory organisation we are committed to ensuring that the identifiable personal information we collect, hold and use will be processed in accordance with legislation, good practice and the expectations of individuals, to meet and ensure security and privacy requirements. This Charter sets out the principles and minimum standards that will underpin the processing and exchange of personal information.

3.2 A list of the organisations that have signed up to this Charter, and have agreed to adopt the principles and standards set out in it can be found on the following link: https://www.nelincs.gov.uk/council-information-partnerships/information-governance/information-sharing/

4 Designated Officer

4.1 Each signatory organisation must have in place a Designated Officer, responsible for approving and monitoring the processing of personal information in accordance with statutory, regulatory and legal obligations.

4.2 For Health and Social Care organisations this will be the Data Protection Officer, Caldicott Guardian or the Senior Information Risk Owner, for organisations signed up to Public Service Networks it will be the Data Protection Officer or Senior Information Risk Officer. For all other organisations it will be a senior officer with responsibility for information governance nominated by the Chief Executive or equivalent.

5 The principles guiding the sharing of information

5.1 As a signatory organisation we will work to:

a) Support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymous information in accordance with our legal, statutory and common law duties, and the requirements of this Charter and other additional guidance as notified to us;

b) Ensure a copy of the Charter and the identity of the Designated Officer are clearly and widely promoted across the organisation and available to all;

c) Have in place effective policies and procedures to meet our responsibilities for the secure and confidential sharing of information, aligned to statutory requirements and this Charter;

d) Ensure that all employees and those acting on our behalf are aware of, understand and comply with their responsibilities for information governance, security, confidentiality and data quality through appropriate promotion, training, monitoring and enforcement.

5.2 When sharing information we will ensure that:

e) Individuals are fully informed about the information held about them and how it will be used and shared;

f) Information will be shared lawfully, fairly and transparently;

g) Only the minimum identifiable information that is required for the purpose is collected and shared. The information shared should be relevant, proportionate and not excessive for specified purpose, and be defined by the appropriate Tier 2 Protocol.

h) Wherever possible statistical, aggregated, anonymous or pseudonymised information is provided, to eliminate the risk of individuals being identified;

i) Information is clearly identified as being fact, opinion, or a combination of the two;

j) Information is only used for the purposes for which it was collected or shared;

k) Information is kept and shared safely and securely, with appropriate safeguards in place to ensure only individuals with a legitimate right have access to it, preventing accidental or deliberate unauthorised access;

l) Information no longer needed for legal or administration requirements is disposed of in a safe and appropriate manner;

m) The capacity of a data subject, including children and vulnerable adults, to exercise their right to provide or refuse consent will be considered on an individual case by case basis; and

n) Considerations of confidentiality and privacy will not automatically cease on death.

6 Tier 2 - Information Sharing Agreements

6.1 The focus of each Tier 2 agreement is the particular **purpose** underlying the need to share information, specifying who is sharing the information, the information being shared and the legal basis for the sharing of information which is documented in Part A. Part B details the processes in place to ensure that the information is securely exchanged and managed in accordance with the legal obligations.

6.2 Tier 2 Agreements will be signed on behalf of each partner by a senior manager, with responsibility for operational delivery.

6.3 Partners will when appropriate upload information sharing agreements to the Information Sharing Gateway.

7 Lawful basis and legal requirements

7.1 The principle legislation and guidance governing the protection and use of personal information is:

a) Data Protection Act 2018;
b) General Data Protection Regulation;

c) Law Enforcement Directive;
d) Human Rights Act (Article 8);
e) Privacy and Electronic Communication Regulations;
f) Freedom of Information Act;
g) Environmental Information Regulations;
h) The Common Law Duty of Confidentiality; and
i) Caldicott Principles

7.2 All partners commit to respect the rights of individuals, following good practice and adhere to legislation in the development and implementation of Information Sharing Agreements.

7.3 The Freedom of Information Act and Environmental Information Regulations gives a general right of access to the information public authorities hold. Any requests for information in relation to the Charter must be processed in accordance with legal and statutory obligations following the established procedures of the partners, were appropriate requests will be processed jointly.

7.4 Requests in relation to Tier 2 Agreements must consider if the disclosure of any elements would compromise the procedures in place for the security and protection of the personal information, and potentially will be subject to an exemption to disclosure.

8 Information Security

8.1 Each signatory will have in place appropriate information security policies and procedures in place to ensure personal, sensitive and confidential data are appropriately protected in accordance with the Data Protection legislation.

8.2 The information security policies and procedures of partners will be informed and where necessary comply with the following standards and guidance:

a) ISO 27001;
b) NHS Data Security and Protection Toolkit;
c) PSN Code of Connection;
d) Government Connect Secure Extranet (GCSX);
e) Health and Social Care Network;
f) DCB1596 (minimum non-functional requirements for secure email service); and
g) Cyber Security Essentials.

8.3 Please see Guidance Note 1 which sets out the minimum standards expected to ensure personal data is appropriately protected to prevent unauthorised access, disclosure, deletion or alteration:

9 Complaints

9.1 Complaints will be processed in accordance with the established procedures of the partners to each agreement, were appropriate complaints will be handled jointly.

10 Monitoring and Review

10.1 As a signatory to the Charter we agree to support the monitoring and review of the Charter through a virtual group set up by the signatories.

11 Partnership undertaking

11.1 As a signatory to the Charter we accept the principles and standards laid down in this document will provide a secure local framework between the signatory organisations for the secure sharing of personal and non-personal information in a manner compliant with legislative and regulatory responsibilities.

11.2 On behalf of the organisation I represent, I confirm that we will undertake to comply with all relevant legislative and regulatory requirements relating to confidentiality, safe information sharing and disclosure, appropriate storage and destruction of information.

Organisation:	
Name:	
Position:	
Signature:	
Date:	

Information Governance contact:	
Name:	
Position:	
Contact e-mail:	

Tier 2 Part A - Information Sharing Agreement

Agreement number	*<insert reference number>*
Review date	*<insert review date>*
Version No.	*<insert version number>*

<Insert agreement title>

1. Parties to this agreement

Organisation name	ICO Registration Number

2. Purpose of the agreement

This agreement creates a framework for the secure, lawful and confidential sharing of personal and non-personal data and intelligence in accordance with the principles and standards defined in the Humber Information Sharing Charter, between the parties to the agreement listed in section 1, for the purpose of *<insert a brief description of the purpose the information will be used for that will assist transparency and public understanding see Guidance Note 2 for examples, it may be easier to bullet point where there are multiple related purposes>*.

The following activities will be undertaken using non-personal data (aggregated or anonymised)

- Managing and planning overall service delivery
- Performance Management
- Identifying best practice

Data provided in a de-identified form (i.e. aggregated or anonymised) must not be knowingly or recklessly re-identified without the express consent of the data controller responsible for the de-identification.

3. The personal data to be shared

3.1 *<insert the name of partner>* will share the following information as part of this agreement

<insert brief description of relevant data sets or data being shared i.e. NHS number, name, address, date of birth, sex, etc.>

Insert additional descriptions as required

A more detailed description of the information being shared can be found in the individual Data Set Lists.

4. The basis for the sharing of personal information

This section explains the basis for the fair and lawful sharing of data in accordance with this agreement. If you are a public sector body, you may be under a legal duty to share certain types of personal data. Even if you are not under any legal requirement to share data, you should explain the legal power you have which allows you to share. If you are a private or third sector organisation then you may not need a specific legal power to disclose personal data, but your agreement should still explain how the disclosures comply with Data Protection legislation.

If consent is to be a basis for disclosure, then your agreement should detail how consent is obtained and address issues surrounding the withholding or retraction of consent. **Please note for public authorities consent will not be a viable basis for processing in almost all cases.**

Please specify the lawful basis for processing (i.e. Article or Schedule in the General Data Protection Regulation, Law Enforcement Directive and Data Protection Act 2018):

If consent is the basis for disclosure, please detail how consent is obtained and how issues surrounding the withholding or retraction of consent are addressed:

Further information about the basis for processing can be found on the ICO's website

5. Implementation, review and termination of the agreement

a) This agreement comes into force from *<insert relevant date or date signed>*

b) This agreement applies *<see Guidance Note 3>*

c) This agreement will be reviewed *at least annually*, the date of the next review is *<insert date>*

d) In the event of a data incident, the identifying partner will notify all partners listed in section 1 and the incident will be investigated following their established procedures and reported to the ICO if required under the General Data Protection Regulation.

e) Termination of this agreement must be in writing giving at least 30 days notice to the other partners.

f) If the partners to this agreement change, the agreement must be reviewed and updated by all participating parties. Partners leaving the agreement must review the data provided to it under this agreement to ensure compliance with legal obligations, such as information is only retained for as long as is necessary and it is disposed of in a secure manner.

g) Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its subcontractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with this agreement.

h) Monitoring and Due Diligence of this agreement will be undertaken in light of each partners established procedures.

6. Processing of personal information

6.1 Personal information will be shared and processed by all partners in accordance with Data Protection legislation and where applicable the Caldicott Principles.

6.2 The Record of Processing Activities and Privacy Notice(s) of each partner must reflect the processing of personal information under this agreement as required by Data Protection legislation.

6.3 Only the minimum necessary personal information relevant to the specified lawful and fair purpose will be shared and where possible aggregated or anonymised non-personal data will be used.

6.4 The information shared must meet agreed standards of accuracy and quality.

6.5 The information must be securely disposed of when no longer required for the purpose(s) it was shared for or to meet any legal or audit obligation

6.6 Information will only be accessible to those individuals who are authorised to receive it and is necessary for their role.

6.7 Appropriate information governance and security training supported by ongoing awareness activities will be provided to all individuals acting on behalf of partners.

6.8 Any information shared under this agreement, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) except as required under statute or regulation, or under the instructions of a court.

6.9 The rights of data subjects and others including Subject Access Requests, complaints or notices to prevent processing will be handled in accordance with applicable legislation and established procedures. If appropriate other partners will be informed of requests received.

7. Declaration

I agree to accept responsibility for the execution of the terms of this agreement and to ensure all relevant legislation is complied with in the processing of personal information.

Name:	
Organisation:	
Position:	
Signature:	
Date:	

Additional signatory boxes can be added if required, or parties can sign separate copies.

Tier 2 Part B - Information Sharing Agreement - Data set list

Agreement number		Data List number	

1. Parties sharing information

Party disclosing information	
Party receiving information	

2. Information sharing purpose and lawful and fair basis

2.1 The specific purpose information is being shared for:

2.2 The lawful and fair basis for the sharing of the information is:

2.3 If the information being processed under this agreement is personal data of individuals accessing health and social care services, have all parties attained the mandatory level of the NHS Data Security and Protection Toolkit?	Yes		No		N/A	

3. Description of the information being shared

3.1 If the information being shared is a specific system module or a report, please provide a description of the relevant module or report below:

3.2 Alternatively please provide details of the data items being shared in the table below:

No.	Data item	Data description (see Guidance note 4a)	Format of data (see Guidance note 4b)
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			

<insert additional lines if required>

3.3 Does the receiving partner become the Data Controller on receipt of the information?	Yes		No	

3.4 Has a Data Protection Impact Assessment been undertaken?	Yes		No		N/A	

4. Information quality

4.1 Will any quality checks be applied to the data prior to sharing under this agreement, additional to those normally undertaken by the disclosing partner?	Yes		No	

<Please provide details of additional quality checks here>

4.2 Partners receiving shared information are responsible for applying relevant quality assurance before using the information.

4.3 Any discrepancies with the data should be reported to all parties immediately on discovery.

5. Secure transfer of information (to be completed by party disclosing the information)

5.1 The trigger for the secure sharing of information under this agreement
<What criteria must be met in order for information to be shared - examples include at an agreed time period such as weekly, monthly quarterly; on request from receiving partner; or data subject milestone or action such as reaches specific age, accesses a service>

5.2 Method of recording the disclosure, sharing or access to information under this agreement
<Insert the business procedures in place to record the sharing of information, such as audit trials or disclosure logs>

5.3 Arrangements in place for the secure exchange of information
<Detail all the controls and business procedures in place for the secure exchange of information; examples include system access controls, encrypted USBs, secure e-mails, personal or courier delivery>

6. Secure receipt of information (to be completed by party receiving the information)

6.1 Arrangements in place for the secure receipt and storage of information
<Detail all the controls and business procedures in place for the secure receipt and ongoing storage of the shared information; examples include system and physical environment access controls>

6.2 Who will be authorised to have access to the information
<Detail as a minimum the team name and job title of the officers authorised to access the information. Where appropriate individual officers should be named>

7. Breaches

7.1 In the event of a data incident, partners will follow their own reporting, investigation and disciplinary procedures and if required report to the ICO within 72 hours.

7.2 Details of confidentiality and data incidents will be notified to the point of contact of the other partner(s) identified in section 1 of the Data List within *<insert timescales>*

8. Retention and Disposal (to be completed by party receiving the information)

8.1 The retention period for the shared information is:

<This section should detail the timescales for the receiving partner to review the shared information to determine if they need to continue to hold it >

8.2 The disposal method for the shared information when no longer required is:

<This section should detail the arrangements the receiving partner must follow for the disposal of the shared information when it is no longer necessary for them to hold the information >

8.3 Will the disclosing partner be informed when the data is disposed of?	Yes		No	

<If yes, please detail how this will be done>

9. Point of Contact with operational responsibility for the data

I agree to accept responsibility for the execution of the terms of this agreement and to ensure all relevant conditions and legislation is complied with in the processing of personal information.

Name:	
Disclosing Party:	
Position:	
Signature:	
Date:	

Name:	
Receiving Party:	
Position:	
Signature:	
Date:	

Guidance Notes

Note 1) Information Security standards: The minimum standards to ensure personal data is appropriately protected to prevent unauthorised access, disclosure, deletion or alteration include:

a) Unauthorised officers and other individuals are prevented from gaining access to personal data;
b) Visitors must be supervised at all times;
c) All electronic systems containing personal data must be password-protected, to prevent unauthorised access;
d) Passwords must be treated as private to the individual and NOT disclosed to others;
e) All electronic devices including PCs, laptops and smartphones must be 'locked' when unattended or not in use;
f) All personal data stored on mobile electronic devices such as laptops, USBs, smartphones etc., must be protected by encryption;
g) All resources (including mobile devices, printouts) containing personal data must be placed in secure locations when not in use, and only accessible to authorised officers;
h) Anti-virus checks are undertaken on software / removable media prior to use on networks / machine;
i)
j) Data and documents are classified to indicate their sensitivity (in terms of the likely impact resulting from compromise, loss or misuse) and marked appropriately when necessary i.e. OFFICIAL - SENSITIVE. Further guidance can be found in the Government Protective Marking Classification Scheme; Caution is exercised in the use of e-mail, recipients are checked and personal data is only exchanged using secure e-mail;
k) Caution is exercised in the use of fax communications, the intended recipient of a fax containing personal data must be aware that it is being sent and has ensured security on delivery;
l) Where personal data is removed from a secure environment, appropriate security measures must be in place to keep it secure and protected;
m) Caution is exercised in the use and transport of personal data outside of its secure environment or in the public domain to prevent loss or unauthorised disclosure;
n) Information must be disposed of securely; and
o) Personal data must not be disclosed to anyone other than the data subject unless you have their consent, or it is a registered disclosure, required by law, or permitted by Data Protection legislation.

Note 2) Examples of the purpose for which information is shared includes

a) For the detection and prevention of crime including Facilitating a co-ordinated approach that targets crime and disorder
b) For the administration of Housing Benefit - To assess and validate entitlement
c) To deliver a particular service or outcomes
d) Managing the cost effective and appropriate allocation of resources to meet the needs of the data subject

Note 3) Examples of the purpose for which information is shared includes

a) whilst the purpose specified in section 2 remains lawful and fair and is necessary to meet business or legal obligations.
b) until a specified date, which should be inserted.
c) until a specified criteria is achieved, details of which should be inserted i.e. end of a contract or project.

Note 4) All parties to the agreement must ensure that there is a common understanding of the data to be provided / received.

Point 4a: The Data description should provide a clear definition of the data item. For example: **Contact Name = the name of the client's carer (usually relative or family friend) who may be contacted by professionals.**

Point 4b: The Format of data should provide a clear description of the format for data item. For example: **Date of Birth = DD/MM/YYYY**