Information Sharing Gateway

Northamptonshire Safeguarding Children Partnership (NSCP) - DS010282 Northamptonshire Safeguarding Children Partnership (NSCP)

Information Sharing Agreement

DF014007

Introduction

The Parties to this Information Sharing Agreement (ISA), except where indicated under "Parties to this Agreement", are signatories to the Information Sharing Gateway (ISG) Memorandum of Understanding.

This Memorandum of Understanding sets out the general principles of Information Governance that all organisations who access and use the Information Sharing Gateway have agreed to. It provides a framework for safeguarding the processing of data and information as defined by the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

General Principles

1. All signatories to this MoU agree to process personal information in accordance with their organisation's information governance policies and procedures, or as directed by the standards applicable to the information being processed.
2. Organisations are expected to identify and use appropriate information assurance framework[1] and will commit to complying with the relevant standards within that regime and sharing the evidence of attainment and any associated action plans on request with ISG partner organisations.
3. Each organisation shall have appointed a responsible / accountable officer who will ensure the protection of personal information for example a Caldicott Guardian, Data Protection Officer or a Senior Manager responsible for data protection.
4. Each organisation will be take appropriate organisational and technical measures towards compliance with Data Protection Act 2018, Caldicott Principles, ISO 27001 Series of Information Security Standards, Freedom of Information Act 2000 and national guidance and rules around processing personal confidential information and other relevant legislation.
5. Each organisation is committed to identifying, documenting and risk assessing their data flows with any mitigating actions defined and agreed.
6. Each organisation is committed to ensuring staff are appropriately trained and comply with organisational policies in relation to Information Governance, including Data Protection, Confidentiality, Caldicott Principles, Data Security, Records Management and Freedom of Information.
7. Organisations will promptly notify other partner organisations of any Information Governance breach, vulnerability or threat that could affect the security of the data being shared.
8. Organisations will agree, security clearances permitting, to allow partner or lead organisations, or its representatives, to carry out audits or visits to confirm compliance with agreed assurance requirements.
9. Each organisation commits to ensure that the data is shared in a safe and secure manner meeting the agreed purpose of the sharing and protecting the rights and freedoms of individuals.
10. Any requests for information under the Freedom of Information Act 2000 or the Data Protection Act 2018 should be directed to the original organisation's FOIA Officer/Data Protection Officer.
11. Organisations may not create or establish onward sharing or sharing for an additional purpose without having first established a lawful basis for doing so and having the agreement of the original data controller.

[1] Appropriate information assurance framework for example Data Security and Protection Toolkit, ISO 27001, Public Service Network (PSN), Cyber Essentials

Parties named in this Agreement

The Parties listed below recognise their responsibilities for ensuring this agreement complies with all legislation and other requirements relevant to the personal data being shared, including the specific governance measures set out in this ISA.

Organisation	ISG Status	Senior Officer/Contact
NORTHAMPTONSHIRE CHILDREN'S TRUST (ICO: ZA781861) *Providing and Receiving Data*	MoU Signed: 17/02/2022 Assurance: Expired	Senior Officer: Francis Evans Hannay Org Contact: francis.hannay@NCTrust.co.uk
Chief Constable Northamptonshire Police (ICO: Z4894886) *Providing and Receiving Data*	MoU Signed: 16/05/2022 Assurance: Limited	Senior Officer: Paul Bullen Org Contact: paul.bullen@northants.police.uk
CHILDREN AND FAMILY COURT ADVISORY AND SUPPORT SERVICE (CAFCASS) (ICO: Z5384497) *Providing and Receiving Data*	Not signed up to ISG MOU Assurance: Not submitted	Senior Officer: Org Contact: isla.kaye@suffolk.nhs.uk
EAST MIDLANDS AMBULANCE SERVICE NHS TRUST (ICO: Z8610634) *Providing and Receiving Data*	MoU Signed: 25/02/2019 Assurance: Significant	Senior Officer: Richard Lyne Org Contact: janette.kirk@emas.nhs.uk
KETTERING GENERAL HOSPITAL NHS FOUNDATION TRUST (ICO: Z4936855) *Providing and Receiving Data*	MoU Signed: 07/06/2018 Assurance: Significant	Senior Officer: Neill Bolderston Org Contact: chris.waller3@nhs.net
National Probation Service - North West Division *Providing and Receiving Data*	Not signed up to ISG MOU Assurance: Not submitted	Senior Officer: Org Contact:
NHS NORTHAMPTONSHIRE CCG (ICO: ZA743708) *Providing and Receiving Data*	MoU Signed: 18/07/2022 Assurance: Significant	Senior Officer: Alan Haycock Org Contact: louise.chatwyn@nhs.net
NORTH NORTHAMPTONSHIRE COUNCIL (ICO: ZA928927) *Providing and Receiving Data*	MoU Signed: 05/10/2021 Assurance: Limited	Senior Officer: Adele Wylie Org Contact: neill.bolderston@northnorthants.gov.uk
NORTHAMPTON GENERAL HOSPITAL NHS TRUST (ICO: Z4694847) *Providing and Receiving Data*	MoU Signed: 01/03/2019 Assurance: Significant	Senior Officer: Hugo Mathias Org Contact: Dan.Howard3@nhs.net
Northamptonshire County Council Fire and Rescue Service (ICO: Z7589390) *Providing and Receiving Data*	Not signed up to ISG MOU Assurance: Not submitted	Senior Officer: Org Contact: mainge@northantsfire.org.uk
Northamptonshire Healthcare NHS Foundation Trust (ICO: Z6769102) *Providing and Receiving Data*	MoU Signed: 07/06/2018 Assurance: Significant	Senior Officer: Adam Shelley Org Contact: adam.shelley@nhft.nhs.uk
West Northants Council (ICO: ZA896620) *Providing and Receiving Data*	MoU Signed: 16/11/2021 Assurance: Limited	Senior Officer: Bellinda Cotton Org Contact: Bellinda.Cotton@westnorthants.gov.uk
NORTHAMPTONSHIRE YOUTH OFFENDING SERVICE (ICO: Z2250338) *Providing and Receiving Data*	Not signed up to ISG MOU Assurance: Not submitted	Senior Officer: Org Contact: mhodgson@northamptonshire.gov.uk

Responsible Senior Officers

The Responsible Senior Officers named above provide assurance that:

- The details captured in this Information Sharing Agreement accurately describe the data sharing practices and the controls in place to govern them.
- Their organisation and its staff will make every effort to ensure that the controls are monitored and maintained and data sharing will only happen as described herein.
- Should their organisation wish to deviate from the practices and controls described here, they will review this data flow to ensure that these changes are captured.

Purpose and Justification for Sharing

Purpose

The Parties agree to use shared information only for the specific purposes set out in this document and to support the effective administration, audit, monitoring, regulatory inspection of services and reporting requirements.

The Parties accept that shared information shall not be regarded as general intelligence for the further use by recipient organisations unless that further purpose is defined in this agreement and respective service users have been informed of this intended change of use.

The purpose, specific to this information sharing arrangement, is identified as:

The information shared is intended to cover a number of both operational and review purposes. These include:
a) if there is reasonable cause to suspect children suffering or likely to suffer significant harm under section
47 of the Children Act 1989
b) if a child is in need under Section 17(10)
c) provision of early help and prevention to improve outcomes for children and young people at all stages
of their development
d) prevention and detection of Child Sexual Abuse and exploitation (CSE) offences
e) protection of children who are at risk or who are the victims of Female Genital Mutilation
f) enabling the Northamptonshire Safeguarding Children's Board to meet their statutory duty to conduct Rapid Reviews, Child Safeguarding Practice Reviews and Child Death Reviews.
g) Information requested for the purpose of undertaking health reviews for Looked After Children.

Benefits

The benefits derived from this information sharing arrangement, are identified as:

To assist professionals within the children's workforce when sharing information during the

management of child protection concerns they encounter amongst the children, young people and families they are working with and within the requirements of Northamptonshire Safeguarding Children Procedures.

Restrictions on other use and further disclosure

It is recognised that unless the law specifically requires or permits this, shared information will not be used for different purposes or further disclosed. Even where the law permits further disclosure, in line with good practice the originating data controller will be consulted first and depending on the circumstances, it may be necessary for the data subject to be informed of the disclosure.

The Information Being Shared

Types of Information

The types of information, to be shared under this agreement, are identified as:

- Law Enforcement
- Personal
- Special Category Personal Data

Data Subjects

The data subjects, whose information is to be shared under this agreement, are identified as:

- Advisers, consultants and other professional experts
- Customers and clients
- Offenders and suspected offenders
- Patients
- Relatives, guardians and associates of subject
- Residents
- Students and pupils

Data Fields to be Shared

The Personal data items, to be shared under this agreement, are:

- Address
- Age
- DOB
- Email Address
- Gender
- Home Phone Number
- Income / Financial / Tax Situation
- Living Habits
- Marital Status
- Mobile Phone Number

- Name
- NHS Number
- NI Number
- Other General Identifier
- Photograph
- Physical Description
- Postcode
- Sex

The Special Category data items, to be shared under this agreement, are:

- Criminal Proceedings / Outcomes / Sentence
- Education / Professional Training
- Employment / Career History
- Family / Lifestyle / Social Circumstance
- Financial Affairs
- Offences Committed / Alleged to have Committed
- Physical / Mental Health or Condition
- Racial / Ethnic Origin
- Religion or Other Beliefs
- Sexual Life / Orientation

The other specific data fields, to be shared under this agreement, are:

Name(s) and Alias'
Dates of Birth and Dates of Death (if applicable)
Current Address and Previous Addresses
Contact information and Next of Kin
Family Information regarding siblings
Information on contacts with service/team
Outcomes of contacts
Names of key workers/staff involved
Alleged perpetrator and their relationship to the victim
Health Information (GP/Health Workers involved)
Photos of injuries sustained (in some cases)
Child Protection Plans and associated documentation
Offending and criminal information of data subject, family and associated network.

Information Security & Confidentiality

Organisational and technical measures

The Parties shall take appropriate technical, security and organisational measures against unauthorised or unlawful processing of the personal data and against accidental loss or destruction of, or damage to, personal data.

Data Transfer Modes and Controls

Transfer Mode	Controls
Electronic data transferred via manual system transfer (uploaded or downloaded)	• Via N3 / HSCN secure connection • Secure encrypted FTP • Secure Web Portal
Electronic data accessed on-site by staff working for partner organisations	• Works for a 'trusted' organisations • Confidentiality / non disclosure agreements or similar • Trained and completed competency test for system
Information delivered by voice	
Electronic data transferred by email	• Secure encrypted email • Password protected document • Email address confirmed

Frequency of Exchange	Number of Records
Ad-hoc	Transfer - 11-50

Post Transfer Storage and Security

Physical location and method of storage:

- Server - system on organisation premises

Data security after transfer:

- Area accessed by key / keypad / access card
- Password protection

Access controls after transfer:

- System login

Data Protection Impact Assessment

Lawful basis for sharing personal information

Statutory duty / power to share

The legislation and/or regulations providing a mandatory duty or discretionary express or implied power for each of the relevant public authority partners to this agreement to share personal data for the purposes described in this agreement, are:

Children Act 1989, s17(10) & 47(1)

Sharing on the basis of informed consent

The consent model(s) used for this sharing arrangement is / are:

- Not required - please specify justification / exemption

Exemption reason / justification: Consent is not required as no clear alternative can be provided to data subjects. NCT relies on Article 6(1)(e) - Public Task as the legal basis to process the personal data. NCT, as the provider of statutory children's social services to the Northamptonshire Unitary Authorities, is carrying out a specific task in the public interest which is laid down by law; or exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

GDPR legitimising conditions

The Article 6 conditions relied on for this agreement are:

- Consent of the data subject
- Task carried out in the public interest / authority vested in the controller
- Vital interests of the data subject

The Article 9 conditions relied on for this agreement are:

- Explicit consent of the data subject
- Information has been made public by the data subject
- Necessary for archiving purposes for public interest, scientific or historical research
- Necessary for public functions
- Necessary for public interest reasons in the area of public health
- Vital interest of the data subject or another person

Informing Individuals

The privacy notice / amendments relevant to this data sharing arrangement are:

None specified.

Adequacy, relevance, necessity

The following checks have been made regarding the adequacy, relevance and necessity for the collection of personal and / or sensitive data:

All appropriate checks are carried out in accordance with each participating organisation's organisational and technical procedures.

Provisions for the accuracy of the data

The following provisions have been made to ensure information will be kept up to date and checked for accuracy and completeness by all organisations:

- Assurance in place (e.g. DSP, PSN)
- Staff aware of responsibilities when working with data
- Clear retention schedules

Retention and disposal requirements

The following arrangements have been made to manage the retention and disposal of data by all organisations:

- Assurance in place (e.g. DSP, PSN)
- Policies and procedures which state / define Retention schedules
- Policies and procedures which state / define Disposal methods and criteria

Individual rights

Subject Access Requests for individual records will be dealt with as follows:

- Assurance in place (e.g. DSP, PSN)
- Clearly defined procedures in place for Subject Access Requests for individuals

- Clearly defined procedures in place to handle rectification and blocking of data

Technical and organisational measures

The receiving organisation's policies, processes and standard operating procedures can be described as follows:

- Assurance in place (e.g. DSP, PSN)
- Clearly defined
- Up-to-date
- Readily available
- Understandable (in plain English) for staff to use

The receiving organisation manages incidents according to the following:

- Reviewed including any root cause analysis and action plans

The receiving organisation's training for both the system and data can be described as:

- Assurance in place (e.g. DSP, PSN)
- Users are aware of their responsibilities when using the asset
- Regularly trained and tested on their understanding
- Understand what to do in the event of a breach or incident

The receiving organisation's security control for the asset can be described as:

- Assurance in place (e.g. DSP, PSN)
- Secure connection (e.g. https:)
- Secure access (e.g. password protected)
- Audit trail of interactions

The receiving organisation's business continuity arrangements are:

- Assurance in place (e.g. DSP, PSN)
- Clear business continuity arrangements
- Users are aware of arrangements and appropriately trained
- Regularly reviewed and updated (at least annually)

The receiving organisation's disaster recovery arrangements are:

- Assurance in place (e.g. DSP, PSN)
- Regularly reviewed and updated (at least annually)
- Electronic part of a disaster recovery testing regime, regularly tested

The third party / supplier contracts contain all the necessary Information Governance clauses including information about Data Protection (2018) and Freedom of Information (2000):

Yes

Risk Assessment

Description	Controls	Initial Rating	Actions	Final Rating
There are no updates / amendments to the host organisations Privacy Notice	Controls in place	Low	Accept / tolerate	Low
The assurance of one or more of your Partner organisations named in this data flow has either expired, is limited or hasn't been submitted within the system. It is recommended that data sharing partners provide significant assurance on their practices or provide evidence to support assurance. You should ensure that the necessary due diligence and checks are made.	Missing controls: • all partner organisations should have significant assurance or provide evidence to support assurance.	High	Accept / tolerate Partner organisations named in this data flow that are noted as assurance being either expired, is limited or hasn't been submitted within the system are able to demonstrate appropriate levels of assurance or are working to an agreed DSPT Action Plan.	Low
All of the recommended controls are in place to provide assurance of the data being delivered by staff.	Controls in place: • Delivered to intended recipient or department • Delivery staff are aware of their responsibilities • Secure trolley / package used to transfer the data • Package not left unattended	Low	Accept / tolerate	Low
Controls are in place to ensure that the data is transferred in a safe and secure manner by standard post.	Controls in place: • Sent using Special Delivery • Sent using Signed for 1st / 2nd class	Low	Accept / tolerate	Low
Manual electronic transfer is taking place over a controlled platform. Security controls should still be implemented and maintained.	Controls in place: • Via N3 / HSCN secure connection • Secure encrypted FTP • Secure Web Portal	Low	Accept / tolerate	Low

Staff must be appropriately trained and understand their responsibilities when accessing data and be able to demonstrate this. Not all of the recommended controls are in place.	Controls in place: • Works for a 'trusted' organisations • Confidentiality / non disclosure agreements or similar • Trained and completed competency test for system Missing recommended controls: • Honorary Contract	Significant	All partner organisations are able to demonstrate appropriate mandatory training compliance requirements of employees to ensure that they understand their responsibilities when accessing data. Training is completed as part of initial induction and renewal of certification on a regular basis. Honorary Contracts are not believed to be necessary. Partner organisations are not required to have access to NCT systems for the purposes of this data share. Where partner organisations do have access to NCT systems for other purposes, i.e. Police for MASH partnership, their use of NCT systems is strictly limited to the agreed purpose for which access was authorised by NCT and is not to be used for other purposes.	Low
Not all of the recommended controls are in place to provide assurance of the information being delivered by voice.	Controls in place: • Contact number verified and consent checks made • Delivered to intended recipient or department • Recipient(s) work for trusted organisation Missing recommended controls: • Secure / private	Significant	Accept / tolerate The recommendation for a secure/private meeting location or sent and received in a 'Safe Haven' is not regarded as a necessity. NCT premises are secure and only accessible through security pass. All staff must complete mandatory data protection training and	Low

	meeting location or sent and received in a 'Safe Haven'		be aware of the circumstances and environment within which they are disclosing personal information in the course of their duties.	
Servers hosted within the UK are bound by UK Law and legislation. You must ensure that the necessary due diligence and checks are made. Make sure access is controlled.	Controls in place: • Server - system on organisation premises • Off site server - UK based	Low	Accept / tolerate	Low
At least one control is in place which enables the information to be accessed securely in the receiving organisation.	Controls in place: • System login	Low	Accept / tolerate	Low
At least one control is in place which enables the information to be accessed securely in the receiving organisation.	Controls in place: • Area accessed by key / keypad / access card • Password protection	Low	Accept / tolerate	Low
All of the minimum recommended controls are in place relating to the accuracy and completeness of the data.	Controls in place: • Assurance in place (e.g. DSP, PSN) • Staff aware of responsibilities when working with data • Clear retention schedules	Low	Accept / tolerate	Low
All of the minimum recommended controls are in place relating to the retention and disposal of the data.	Controls in place: • Assurance in place (e.g. DSP, PSN) • Policies and procedures which state / define Retention schedules • Policies and procedures which state / define Disposal methods and criteria	Low	Accept / tolerate	Low
All of the minimum recommended controls are in place relating to subject access requests	Controls in place: • Assurance in place (e.g. DSP, PSN)	Low	Accept / tolerate	Low

access requests.	• Clearly defined procedures in place for Subject Access Requests for individuals • Clearly defined procedures in place to handle rectification and blocking of data			
Policies, processes and standard operating procedures for the asset / data are clearly defined, up-to-date, understandable and readily available.	Controls in place: • Assurance in place (e.g. DSP, PSN) • Clearly defined • Up-to-date • Readily available • Understandable (in plain English) for staff to use	Low	Accept / tolerate	Low
Incidents are reviewed appropriately.	Controls in place: • Reviewed including any root cause analysis and action plans	Low	Accept / tolerate	Low
Users of the data are regularly trained, aware of their responsibilities and understand what to do in the event of breach.	Controls in place: • Assurance in place (e.g. DSP, PSN) • Users are aware of their responsibilities when using the asset • Regularly trained and tested on their understanding • Understand what to do in the event of a breach or incident	Low	Accept / tolerate	Low
The asset / data is secure, controlled and interactions recorded.	Controls in place: • Assurance in place (e.g. DSP, PSN) • Secure connection (e.g. https:) • Secure access (e.g. password protected) • Audit trail of interactions	Low	Accept / tolerate	Low
Business continuity arrangements are clear	Controls in place:	Low	Accept / tolerate	Low

arrangements are clear, users are aware and trained with regular reviews and updates.	• Assurance in place (e.g. DSP, PSN) • Clear business continuity arrangements • Users are aware of arrangements and appropriately trained • Regularly reviewed and updated (at least annually)			
Disaster recovery arrangements are in place with regular review and testing where appropriate.	Controls in place: • Assurance in place (e.g. DSP, PSN) • Regularly reviewed and updated (at least annually) • Electronic part of a disaster recovery testing regime, regularly tested	Low	Accept / tolerate	Low

Commencement, Termination and Review

This agreement will be reviewed every 12 months post commencement unless an earlier review for policy or legislative reasons is necessary.

The start date for this agreement is:

To be defined.

The scheduled review date for this agreement is:

To be defined.

This ISA shall be effective from the start date indicated above and shall continue in force until such time as the data sharing ends, this ISA is terminated by either Party, or this ISA is replaced by a new one.

Signatories