

**OFFICIAL**



**SCOTTISH  
FIRE AND RESCUE SERVICE**  
Working together for a safer Scotland

# Overarching Memorandum of Understanding

**HIGHLAND MULTI AGENCY INFORMATION  
SHARING PUBLIC PROTECTION**

**2023**

**OFFICIAL**

**Contents**

**1 Parties, Scope and Purpose..... 3**

    1.1 *Name and details of the parties who agree to share information ..... 3*

    1.2 *Business and legislative drivers. .... 3*

**2 Description of the type of information to be shared ..... 7**

**3 Information Sharing Agreements governance arrangements..... 7**

**4 Overarching fair processing arrangements..... 10**

**5 Data Subjects’ Rights. .... 10**

**6 Overarching security arrangements..... 10**

**7 International transfers of personal data..... 11**

**8 Implementation of the Overarching Memorandum of Understanding..... 12**

    8.1 *Dates when information sharing commences/ends..... 12*

    8.2 *Overarching training and communications arrangements. .... 12*

    8.3 *Overarching publication and transparency arrangements. .... 13*

    8.4 *Non-routine information sharing and exceptional circumstances ..... 13*

    8.5 *Monitoring, review and continuous improvement ..... 13*

    8.6 *Sharing experience: fora and communications. .... 14*

**9 Sign-off ..... 14**

**Document Version History**

**Appendix 1**

## **1 Parties, Scope and Purpose**

### **1.1 Name and details of the parties who agree to share information**

Legal name of parties to MOU	Short name of the party	Head Office address	ICO Registration
Highland Health Board	NHS Highland	Assynt House, Beechwood Park, Inverness IV2 3BW	Z5634253
The Highland Council		Glenurquhart Road, Inverness IV3 5NX	Z5442561
The Chief Constable of the Police Service of Scotland	Police Scotland	Tulliallan Castle, Kincardine, Fife FK10 4BE	Z3611656
The Deputy Chief Fire Officer of the Scottish Fire and Rescue Service	Scottish Fire and Rescue Service (SFRS)	Westburn Drive, Cambuslang, Glasgow G72 7NA	Z3555625

### **1.2 Business and legislative drivers.**

There is an increasing emphasis on multi-agency working in relation to public protection, which requires the parties to share amongst them necessary, relevant, adequate, and proportionate information to enable them to provide co-ordinated and seamless services and perform statutory duties.

Information sharing must take place within a legal and secure framework that also takes cognisance of the respective professional needs and responsibilities of the parties.

To help ensure effective multi-agency working and compliance with statutory and legislative requirements for information sharing including the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulations (UK GDPR), the Human Rights Act 1998, the common law duty of confidentiality, relevant professional codes of conduct/practice, the Caldicott Principles and the Information Commissioner's Data

**OFFICIAL**

Sharing Code of Practice, the parties agree to adopt and implement a two stage framework (the “Framework”).

This memorandum of understanding (MOU) is the first stage of the Framework and sets out the parties’ overarching approach to information sharing for public protection.

Sitting under this MOU will be second stage Information Sharing Agreements (“ISAs”) for each area/context for systematic (regular and planned) information sharing amongst all the parties to this MOU with supporting staff instructions/procedures/guidelines and appropriate policy document as needed.

In adopting the Framework, the parties want to ensure a clear and consistent approach to information sharing amongst them and engender confidence in both staff and the public in the way that they manage multi-agency information sharing.

It is recognised that some public protection arrangements may involve information sharing with bodies/organisations other than the parties to this MOU and who may not have signed up to the Framework. Where this is the case then the parties will endeavour to seek the agreement of those other bodies/organisations to the adoption of the Framework, but the parties will in any event ensure that necessary, relevant, adequate, and proportionate information sharing takes place within a legal and secure framework by entering appropriate Memoranda of Understanding and/or ISAs as needed.

**1.2.1 Purpose of the information sharing**

Purpose description	Primary or secondary purpose
Safeguarding and protecting the public (adults and children) from harm in line with statutory duties.	Primary
Improving the quality, consistency, and effectiveness of services.	Primary
Supporting joint planning, development, and delivery of services.	Secondary

Supporting statutory duties including reporting.	Secondary
Supporting audit, monitoring and inspection of services.	Secondary
Purpose description	Primary or secondary purpose
Supporting national and local initiatives on multi-agency working.	Secondary
Preventing and detecting crime.	Secondary

From the above general purposes, the specific purposes applicable to each party, area/context for systematic information sharing will be detailed within individual ISAs.

Information will be shared only with those authorised and with a need to know.

Indicate how the parties will decide upon changes in the purposes of the sharing	Jointly or independently
	Jointly

Changes in the purposes of the information sharing will be discussed at the Highland Information Sharing Working Group (HISWG), agreed by the Highland Public Protection Chief Officer Group (HPPCOG) and documented by way of an update to this MOU.

### **1.2.2 Legal basis for the processing and constraints**

Information sharing within the scope of this MOU will typically be undertaken under UK GDPR Article 6(1)(e) as sharing is necessary for the performance of tasks carried out in the public interest.

However, other legal bases within that article may be relied upon depending on the situation: -

(1)(a) sharing is based on consent from an individual for a specific purpose<sup>1</sup>;

(1)(c) sharing is necessary to comply with a legal obligation; and

(1)(d) sharing is necessary to protect someone's vital interests.

Where the information to be shared is sensitive (special category) data and/or criminal offence data, additional conditions set out in UK GDPR Article 9 and 10, must be met, and where applicable, the associated condition(s) in UK law, set out in Schedule 1 of the DPA 2018.

Information sharing within the scope of this MOU may also be undertaken under S35(2)(b) DPA 2018 where sharing is necessary for the performance of a task carried out for law enforcement purposes (which purposes are defined in s31 DPA 2018) and is based on law i.e., processing is authorised by either statute, common law or royal prerogative, or by or under any other rule of law. Additional conditions for sharing sensitive personal information set out in s35(5) DPA 2018 must be met, and where applicable, the associated condition(s) in UK law, set out in Schedule 8 of the DPA 2018.

The specific applicable legal basis(es) for each party and each purpose for systematic information sharing and any associated conditions that are met for any sensitive, special category and/or offence data to be shared will be detailed within individual ISAs.

In addition to the legal bases under the DPA 2018 and UK GDPR, information sharing within the scope of this MOU must otherwise be lawful. Full consideration will be given to each party's respective legal obligations/powers when considering and preparing ISAs. Information will not be shared if it is in some other way unlawful.

When sharing children's information within the scope of this MOU, the primary consideration will be the best interests of the child.

Information that is shared will only be used for the specific purpose(s) for which it was shared (unless changes in purposes have been agreed in line with 1.2.1 above), will be stored securely, and deleted when no longer required for that purpose unless it forms part of the recording process of the party's primary role.

---

<sup>1</sup> Police Scotland will not use 'Consent' as a basis for sharing

## **2 Description of the type of information to be shared**

The parties may share relevant, proportionate, and appropriate personal information, sensitive personal information, and criminal offence data.

Personal information is information which relates to a living identified or identifiable individual, including their image or voice, which enables them to be uniquely identified from that information on its own or from that and / or other information available to the recipient of such information

Sensitive (special category) personal information is personal information which:

- reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership,
- concerns health, a person's sex life or sexual orientation.
- is genetic or biometric data.

Criminal offence data is personal data relating to criminal convictions and offences or related security measures. This includes information about alleged commission of offences, proceedings for offences and disposal of such proceedings, including sentencing.

All information to be shared and detailed within individual ISAs must be the minimum necessary to fulfil the purpose of the ISA and be accurate, up to date and timely.

## **3 Information Sharing Agreements governance arrangements**

This section sets out how ISAs and staff instructions/ procedures/ guidelines/appropriate policy documents (if any) will be developed and sets out the approval structures for these.

ISA working groups (ISAWG) will be established by the parties for each area/context where the need for an ISA is identified.

The ISAWG will include representatives from each party to the ISA who have a good understanding of the data flows and the business requirements. They will be assisted by Data Protection Officer(s), Information Security Officer(s), information Assurance

**OFFICIAL**

team, Caldicott Guardian, Legal Advisers and relevant professional bodies as required, depending on the complexity of the agreement.

The ISAWG will ensure that : -

1. Where necessary, **Data Protection Impact Assessments** (DPIAs) are undertaken by the parties. A DPIA will aid the exploration, discussion and understanding of risks faced by each party to the ISA and the need for any specific provisions within ISAs to address these and/or specific instructions/guidelines, training, security measures etc.

Other preparatory work/risk assessments e.g., human rights impact assessment or equalities impact assessment, are undertaken as needed following each party's preferred template(s) and taking advice from relevant advisers as needed.

2. **A draft ISA** is prepared following an agreed template and taking account of agreed guidance/instructions and the provisions within this MOU.

The template will help ensure compliance with the Information Commissioner's Data Sharing Code of Practice. ISAWG will need to consider Codes of Practice for specific professional fields and legislation relevant to each context for an ISA.

Provisions from this MOU should not be repeated within ISAs. ISAs must, however, reference this MOU.

The specific applicable legal basis(es) for each party and each purpose for systematic information sharing and any associated conditions that are met for any sensitive, special category and/or offence data to be shared will be detailed within the ISA.

3. Members have undertaken **consultation** with DPOs, legal advisers and relevant professional leads on the draft ISA, if they have not already been involved in the working group.
4. The need for any appropriate **policy documents** has been identified, and if needed, prepared by the relevant party in line with any guidance supplied by the Information Commissioner or where policy documents already exist, they are reviewed and amended if needed.



**OFFICIAL**

Risk assessments relevant to the policy documents e.g., DPIA, human rights impact assessment or equalities impact assessment, will be undertaken as needed following each party's preferred template(s) and taking advice from relevant advisers as needed.

5. Separate sub-working group(s) are established as needed for the preparation/review of any **associated staff instructions/procedures/guidelines**. Participation from operational teams will be vital where these are being considered. Staff instructions/procedures/guidelines must incorporate certain areas, see **Appendix 1** attached.

These can either be in the format of joint instructions or documents agreed amongst the parties or individually within each party but identifying how each parties' procedures will interact/link to enable information sharing rather than a complete set of joint new instructions for staff. Instructions should reference existing documentation as much as possible rather than duplicating or reinventing operational procedures.

Agreement on any specific security controls should be recorded.

All associated staff instructions/procedures/guidelines must be referenced within ISAs.

6. ISAs are submitted for **sign off** to:-
  - a. NHSH – Senior Information Risk Owner (SIRO)/Caldicott Guardian
  - b. THC – Information Asset Owner for functional area
  - c. PS – Divisional Commander, Highlands & Islands Division
  - d. SFRS – Deputy Assistant Chief Officer for the North Service Area

Associated policy documents will be submitted through each parties' individual approval structures before sign off.

Periodic reviews of ISA's will be undertaken by ISAWG's and will follow similar processes to those above for new ISAs.

HISWG will maintain an overview of all ISA work and maintain an up-to-date register listing all ISAs in progress, approved, and signed off, and review dates.

HISWG will report by exception to HPPCOG.

Where issues/disputes arise at an ISAWG, these will be escalated to HISWG and onward by that group as needed to HPPCOG.

#### **4 Overarching fair processing arrangements**

Privacy Notices will be reviewed and updated by each party as needed when any new ISAs are entered into before information sharing starts.

The parties will only share information in ways that people would reasonably expect unless unexpected sharing is justified and not in ways that have unjustified adverse effects on them.

#### **5 Data Subjects' Rights.**

All Freedom of Information (Scotland) Act 2002 requests (FOIs), Subject Access requests under the DPA 2018/UKGDPR and other rights requests received from individuals will in all cases be referred immediately to the information officer/team or equivalent of the party receiving the request/objection as there are strict timescales and various procedural requirements that must be met in dealing with these. These officers/teams will deal with all requests received in accordance with the receiving party's applicable policies and procedures and will be best placed to consider the applicability of any exemptions/restrictions.

If a request is received regarding information relating to or received from another party, the relevant party will be notified of this where appropriate and may be consulted on the response although the final decision remains with the party in receipt of the application. All parties will act and respond timeously given the deadlines involved.

#### **6 Overarching security arrangements.**

The security controls applicable by each organisation will be:

Jointly agreed between the parties

Independently decided by each party

Assessed and established via ISA for each particular contextual sharing

ISAs will also detail relevant security classification of documents (e.g., Government Security Classifications), agreed arrangements for retention, review, and secure disposal of information including the deletion/return of information to the party that supplied it upon the termination of an ISA.

In preparing ISAs any differences in security standards, systems, procedures, and classifications/protective marking systems etc will be considered and appropriate standards etc./actions/safeguards agreed and documented.

All known or suspected breaches of security, confidentiality or other violations will be reported immediately in line with each party's incident reporting procedures and, in the case of reportable personal data breaches, onward as needed to the Information Commissioners Office within 72 hours of it being discovered. Failure to report a reportable personal data breach to the Information Commissioners Office can lead to a fine.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted stored or otherwise processed. These breaches need to be assessed for the likelihood and severity of risk to people's rights and freedoms and if likely reported.

Action should be taken to mitigate any risks arising from security breaches and an investigation will be undertaken by the party concerned to identify where possible the person(s) responsible, what information has been compromised, whether the integrity of any systems have been compromised and any required/appropriate actions. Should the breach of security be deemed to be of a criminal nature then the relevant party must report the event to Police Scotland to enable them to investigate. The party concerned will also report all known or suspected breaches of security to the other parties and address any required actions to provide assurance on ongoing security of information sharing processes.

## **7 International transfers of personal data**

Personal data shared in line with this agreement will be transferred to

EEA countries only

Out with EEA. Please specify the countries:

[ ] Will not be transferred outside the UK

[X] Assessed and established via ISA for each particular contextual sharing

## **8 Implementation of the Overarching Memorandum of Understanding.**

### **8.1 Dates when information sharing commences/ends**

Commences – When each individual ISA is signed off by all parties, associated documentation as needed is in place and appropriate staff awareness raising/training in that area has been undertaken.

Ends – Any party can give to the other parties' six months written notice of termination of this MOU. However, any party may terminate by notice in writing immediately to the other parties' if: -

- 1 another party is in breach of any of the terms of this MOU which, in the case of a breach capable of remedy, shall not have been remedied by that other party within 21 days of receipt of a written notice specifying the breach and requiring its remedy; or

(ii) another party is incompetent, guilty of gross misconduct and/or any other serious or persistent negligence in the carrying out of its duties hereunder.

### **8.2 Overarching training and communications arrangements.**

The parties are responsible for ensuring that all ISAs that they sign are disseminated, understood, and acted upon by all relevant staff.

Training and awareness sessions, including induction and refresher training, will be available for all relevant staff where an ISA/work instructions are agreed and put in place to ensure all staff, current and newly appointed, are clear on their role and processes. Arrangements for this should be considered and set out within ISAs and implemented following their sign off.

Assistance with local training/awareness sessions can be sought from the eHealth Information Assurance & Governance Team at the Scottish Government as required.

Arrangements for communications to data subjects and publishing of information about processing will be considered and set out within ISAs.

### **8.3 Overarching publication and transparency arrangements.**

ISAs may be published on all parties' websites and will be accompanied by additional and easily accessible and easy to understand contextual information, which may be by way of specific privacy notices or otherwise.

Prior to publishing ISAs, the parties will establish if there is any perceived security risk the organisation may be exposed to by publishing specific sections or appendices of the agreement and if a security risk exists, then these portions will be withheld.

ISAs may list all relevant privacy information/notices and where to find them.

### **8.4 Non-routine information sharing and exceptional circumstances**

Information sharing that is done on a regular basis in a routine, pre-planned way will take place in line with agreed ISAs, which should be referred to for guidance.

Information sharing of a one-off, non-routine, exceptional or ad hoc nature that is not covered by an agreed ISA can still take place but should be discussed with relevant line manager(s) and Information Assurance or DPO advice sought as appropriate and as the urgency and seriousness of the situation allows.

### **8.5 Monitoring, review and continuous improvement**

This MOU will be reviewed every 4 years or sooner if the parties agree that an earlier review is needed.

ISAs (including preparatory assessments and any required policy documents) will be reviewed every 2 years by the ISAWG. ISAs will detail when reviews may otherwise be triggered.

Appropriate review periods for work instructions/procedures/guidelines, will be agreed and set out within ISAs.

When reviews are undertaken account will be taken of any changes in the Framework agreed nationally.

ISAs will detail monitoring arrangements.

**8.6 Sharing experience: fora and communications.**

Amongst the parties, HISWG will act as the forum for sharing experiences and HISWG will cascade information to ISAWG's and as needed to HPPCOG.

**9 Sign-off**

Name of Party	NHS Highland	
Authorised signatories	Title /Name	Pam Dudek
	Role	Chief Executive
Head Office address	Assynt House, Beechwood Park, Inverness IV2 3BW	
ICO Registration	Z5634253	

Name of Party	The Highland Council	
Authorised signatories	Title /Name	Derek Brown
	Role	Chief Executive
Head Office address	Glenurquhart Road, Inverness IV3 5NX	
ICO Registration	Z5442561	

**OFFICIAL**

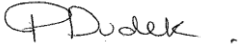

Name of Party	Police Scotland	
Authorised signatories	Title /Name	Chief Superintendent Rob Shepherd
	Role	Divisional Commander
Head Office address	Tulliallan Castle, Kincardine, Fife FK10 4BE	
ICO Registration	Z3611656	

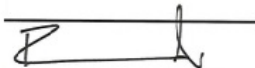

Name of Party	Scottish Fire and Rescue Service	
Authorised signatories	Title /Name	Stephen Wood
	Role	Deputy Assistant Chief Officer
Head Office address	Westburn Drive, Cambuslang, Glasgow G72 7NA	
ICO Registration	Z3555625	

**OFFICIAL**

Sign off

“We the undersigned agree to the details recorded in this Overarching Memorandum of Understanding and are committed to the ongoing monitoring and review of the scope, purpose and manner of the information sharing.”

Signature 		Signature 	
Name	Pam Dudek	Name	Derek Brown
Date	4 March 2024	Date	16 February 2024

Signature 		Signature 	
Name	Rob Shepherd	Name	Stephen Wood
Date	29 February 2024	Date	7 <sup>th</sup> December 2023



<b>Document version history</b>			
<b>Date</b>	<b>Version</b>	<b>Status</b>	<b>Author</b>
16 September 2021	1.0	Initial working draft.	HISWG
01 December 2021	1.1	Subsequent working draft.	HISWG
17 December 2021	1.2	Subsequent working draft.	HISWG
04 August 2022	1.3	Final draft for sign off	HISWG
15 June 2023	1.4	Comments from Police Scotland	
09 October 2023	Final	Final for sign off	

The following sets of instructions must exist, either in the format of joint instructions or existing documents agreed between the parties (e.g. existing local policies and procedures).

- **Sensitivity of information classification**

These instructions should cover details on the sensitivity or other classification of the information within the scope of the ISA, including whether it includes sensitive personal data as defined by the Data Protection Act 2018. Parties can agree to use classifications beyond the minimum required by legislation. Where necessary outlining where there are differences in classification between organisations and issues of equivalency (e.g. between, health, police and central government) and mapping them.

- **Controls over service users**

Controls over service users consist of agreed instructions between the parties on how the information covered by the ISA will be used only by the designated service users for the agreed purposes (e.g. role based access on systems and whether there are enhanced checks/pre-employment screening) and how these users will be designated, authorised, monitored and de-authorised as required. Access to personal data or business confidential information should be based on strict need-to-know basis.

- **Controls over information handling prior and during transmission**

These are a set of agreed instructions, policies, controls and security operating procedures which detail on how information is jointly or independently stored and then prepared for sharing, the mechanisms by which the information is to be shared (e.g. email or file-sharing protocol, tracked mail etc.) and the controls around it (e.g. encryption, tracked mail). If data is to be shared digitally also reference if any shared ICT wide area network is to be used (e.g. Scottish Wide Area Network (SWAN) or Public Services Network (PSN)) and controls needed to safe-guard confidentiality, integrity and availability of information.

- **Controls over information handling after transfer**

These controls record and manage how the recipients of the information will then process, store, delete the information which originated from outside the organisation. Note: once an organisation has shared its information externally with another data

controller it often has little or no actual control over how the partner organisation then stores or uses the data. The ISA and instructions are a means of obtaining some assurance here (but ultimately it is the Data Controller who is responsible).

- **Maturity level of security in organisations sharing information**

This instruction details information about the maturity level of security in the organisations and any equivalency (e.g. both parties have data centres certified to ISO-27001; HMG Security Policy Framework; NHSS Information Security Policy Framework; both parties signed up to PSN Code of Connection etc.) and the agreed procedures to assess this maturity, monitor and communicate changes on the maturity status between the parties.

- **Relevant information security and handling policies and procedures**

All relevant security policies for the information that is to be shared should be listed in the relevant appendix of the ISA. Note: participating organisations may have very different policies (e.g. social media, email, online tools, devices etc.) so it will need to be agreed which operating instructions should be used and to document any agreed “bridge” or mapping instructions between local procedures and policies.

- **Audit trails and accountability**

These are instructions detailing controls on how the information sharing activities are covered by any audit trails that can identify a) which party carried out the activity such as viewing or modifying data; b) non-repudiation in event of a negative event and c) any monitoring to establish and success and security of the information sharing operations.

- **Incidents and reporting**

These consist of a description of the mechanism by which incidents and issues are reported in regard to the information within scope of the ISA (e.g. to a designated person for one or all of the parties etc.). It is also important to specify the circumstances where there needs to be external reporting (e.g. regulators such as Information Commissioner’s Office in the case of personal data; the Scottish Government or other organisation with oversight).

- **Relevant information and record management policies and procedures**

This includes the records management policies and procedures relevant to the information being shared under the ISA. The instructions will identify the retention schedule of the partner organisation and how this will be deployed (for example manual or automatic) and any mechanisms which are in place for archiving or transfer of records to other bodies for example the National Records of Scotland. In scenarios where data controllers access a pool of shared information it is important to specify retention schedules which meet the legislative and business requirements of the organisations involved.

- **Access to information legislation, intellectual property and compliance**

This refers to additional instructions or details beyond the agreements expressed in the ISA, e.g. local procedures on how each relevant party deals with Subject Access Requests (in accordance with DPA), Freedom of Information (Scotland) Act 2002 (and subsequent amendments) or Environmental Information (Scotland) Regulations 2004 (and subsequent amendments) information requests will be managed by the parties in accordance with the processes of the relevant organisation. (For example a request for information created by National Health Services Scotland (NHSS) and then shared with a local authority is likely to be managed, in the first instance, by NHSS). If Intellectual property rights or copyright are relevant, describe whether access to shared information carries any obligations to the originator / owner of that information.