

# Grampian Data Sharing Partnership

## MEMORANDUM OF UNDERSTANDING FOR THE SHARING OF INFORMATION

(to be supported by Individual Information Sharing Protocols)

Aberdeen City Council  
Aberdeenshire Council  
The Moray Council  
Grampian Health Board  
Grampian Police





## **TABLE OF CONTENTS**

- 1.0 PARTIES TO THE MEMORANDUM OF UNDERSTANDING (MOU)
- 2.0 INTRODUCTION
  - 2.1 Scope
  - 2.2 Background
  - 2.3 Data Sharing Principles
- 3.0 OBJECTIVES
  - 3.1 Purpose of the MOU
- 4.0 KEY LEGISLATION & GUIDANCE
  - 4.1 Data Protection Act 1998 (DPA 1998)
  - 4.2 Data Controller
  - 4.3 Subject access requests
  - 4.4 Data subjects rights
  - 4.5 Disclosure to third parties
- 5.0 PURPOSES FOR WHICH INFORMATION WILL BE SHARED
- 6.0 MANAGING INFORMATION SHARING
  - 6.1 Processing conditions for schedule 2 (DPA)
  - 6.2 Processing conditions for schedule 3 (DPA)
  - 6.3 Consent
- 7.0 DATA QUALITY
- 8.0 ACCESS AND SECURITY PROCEDURES
  - 8.1 Transfer of Personal Data
  - 8.2 Use of Personal Data for purposes other than those agreed
  - 8.3 Restrictions on the use of statistical & anonymised data
- 9.0 SECURITY FOR SHARED SYSTEMS
  - 9.1 Recording of individual data
- 10.0 MOU & ISP MANAGEMENT PROCEDURES
  - 10.1 Formal Approval and Adoption
  - 10.2 Monitoring and Review Of ISPs
  - 10.3 Resolving Issues Associated with this MOU & the Individual Protocols
- 11.0 AUDIT
- 12.0 CONTRACTUAL AGREEMENT
  - 12.1 Undertaking
  - 12.2 Data Protection Notification & Control
  - 12.3 Duration & Variation
  - 12.4 Mutual Indemnities
  - 12.5 Alternative dispute resolution
  - 12.6 Definitions

## 12.7 Governing Law

Schedule Part A	Principles of the Data Protection Act 1998
Schedule Part B	Dictionary of Definitions
Schedule Part C	Other Key Legislation
Schedule Part D	Cases of Uncertain Capacity: Children

## 1.0 PARTIES TO THE MEMORANDUM OF UNDERSTANDING (MOU)

1.1 This MOU is a **legal agreement** between

**Grampian Health Board** (also known as NHS Grampian) a body corporate established under the National Health Service (Scotland) Act 1978 (as amended) and having its Head Office at Summerfield House, Eday Road, Aberdeen, AB15 6RE (hereinafter referred to as NHSG). Data Protection Registration Number Z8547986.

**Aberdeen City Council**, a local authority constituted under the Local Government etc (Scotland) Act 1994 and having its Head Office at Town House, Broad Street, Aberdeen, AB10 1FY (hereinafter referred to as ACC). Data Protection Registration Number Z5018566.

**Aberdeenshire Council**, a local authority constituted under the Local Government etc (Scotland) Act 1994 and having its Head Office at Woodhill House, Westburn Road, Aberdeen, AB16 5GB (hereinafter referred to as AC). Data Protection Registration Number Z6501842.

**The Moray Council**, a local authority constituted under the Local Government etc (Scotland) Act 1994 and having its Head Office at Council Office, High Street, Elgin IV30 9TL (hereinafter referred to as TMC). Data Protection Registration Number Z7512703.

**Grampian Police**, a police force constituted by the Police (Scotland) Act 1967 and having its principal office at Grampian Police Force Headquarters, Queen Street, Aberdeen AB10 1ZA (hereinafter referred to as GP). Data Protection Registration Number Z4895344.

who are collectively referred to as "*the partners*". This shall include any statutory successors to the partners.

1.2 Third Party Organisations will be expected to adhere to this MOU as part of their Service Level Agreements or other working relations with the partners.

## 2.0 INTRODUCTION

2.0.1 Legislation and practice in relation to the collection, storage, and sharing of information about data subjects are underpinned by accepted principles.

2.0.2 Confidentiality of personal data is at the centre of these principles. However, if there is reasonable concern that a data subject is at risk of harm this will normally override any requirement to keep information confidential.

All partners have a legal obligation to ensure that a data subject, whose safety or welfare is at risk, is protected from harm.

## **2.1 Scope**

- 2.1.1** The partners have agreed to adopt a two level approach to the management of sharing information amongst the partners.
- 2.1.2** This MOU for the Sharing of Information covers the main principles and purposes for which information sharing is carried out amongst the partners. This MOU encapsulates national and legal requirements.
- 2.1.3** In every context where pre-specified, regular or bulk information sharing takes place an individual information sharing protocol (ISP) will support this document. The ISPs set out specific arrangements, designated responsibilities and additional requirements associated with the specific application.
- 2.1.4** A key benefit of this approach is that for each specific information sharing arrangement, the development of an ISP will facilitate the concentration of resources on the development of practical policies and procedures. As a result, principles agreed within this MOU will not require to be re-defined within the ISPs.

## **2.2 Background**

- 2.2.1** The aim of public policy is that citizens receive the appropriate services which they require. The organisation of these services should not impede or devalue the service provided. This aim clearly requires the partners to work effectively and efficiently together, in order to tailor the specific services to the particular circumstances of each data subject. Sharing information with respect to data subjects amongst the partners is vital to the provision of co-ordinated and seamless services.
- 2.2.2** There have been both real and perceived barriers to information sharing. These may be linked to the legal requirements or ethical standards which require to be satisfied. On some occasions these impediments have focused on personal, inter-professional and inter-organisational mistrust; on worries about responsibility and accountability for personal data; on the absence of enabling mechanisms; and on technical matters. Where information sharing has occurred, its value has often been reduced by misunderstandings in the use of language or inefficiencies in the communication channel. These barriers have led to concerns and to uncertainties regarding the circumstances of information sharing.
- 2.2.3** This MOU and the ISPs have been developed to address these concerns.
- 2.2.4** The need to share information between the partners has long been recognised. Comprehensive and coherent security standards require to be adopted to support the implementation of all UK Government and Scottish Government initiatives in this respect.

**2.2.5** This MOU is designed to ensure that the exchange of personal data between partners conforms with applicable laws, and safeguards the rights of the partners and the data subject.

### **2.3 Data Sharing Principles**

**2.3.1** The partners shall apply the presumption that data subjects aged 12 years or older enjoy capacity to give, withhold or modify consent.

**2.3.2** A presumption of capacity shall only be regarded as having been rebutted if the procedures for establishing incapacity laid down in Schedule Part D have been followed.

**2.3.3** It shall be a fundamental principle of this MOU that, sharing of personal data by the partners shall be in accordance with DPA 1998.

**2.3.4** Most information given to the Partners by Service Users (who for the purposes of this section of the Memorandum are defined as Data Subjects) will be confidential. Confidential information is usually information which is not readily available from another source, has been given for specified purposes only and which includes personal data that individuals would not expect to be disclosed.

## **3.0 OBJECTIVES**

### **3.1 This MOU is intended to:**

- Set out the principles which underpin the sharing of information between the partners;
- Set out the general purposes for which the partners have agreed to share;
- Describe at a high level the procedures which will ensure that information is disclosed in line with statutory and common law responsibilities;
- Describe how this MOU will be implemented, monitored and reviewed.

## **4.0 KEY LEGISLATION & GUIDANCE**

### **4.1 Data Protection Act 1998 (DPA 1998)**

**4.1.1** Since 1 March 2000 the key legislation governing the protection and use of personal data from which a living individual can be identified is the DPA 1998.

**4.1.2** The DPA 1998 covers the standard to be applied when handling information about data subjects and the practices to be followed in order to achieve and maintain those standards. The requirements are set out within the eight data protection principles as provided for within

Schedule 1 of the DPA 1998 (see Schedule Part A). Organisations must comply with these principles in their entirety when handling personal data unless an exemption applies.

## **4.2 Data Controller**

**4.2.1** The partners acknowledge that the 'data controller' is the partner who determines the purposes for which the personal data is collected. This is likely to be the partner that gathers and stores the personal data initially.

**4.2.2** When personal data is gathered on behalf of more than one partner, or shared between partners, each partner may become a data controller jointly and/or in common depending on the particular sharing arrangement involved.

**4.2.3** Individual ISPs made under this MOU will specify which of the partners has the obligation of data controller, and whether that obligation applies to separate personal data or applies jointly and/or in common to shared personal data.

**4.2.4** The partners agree to maintain contact to assist in discharging any obligations laid on a data controller or data processor partner. Unless otherwise specified, contact will be made between each partner's contact designated in the ISPs made under this MOU.

## **4.3. Subject access requests**

**4.3.1** The partners acknowledge that the obligation to respond to subject access requests under section 7 of the Data Protection Act 1998 lies with the data controller.

**4.3.2** A partner that receives a subject access request seeking access to personal data over which that partner and any other partner are data controllers will seek the permission of all relevant data controllers before disclosing the personal data to the data subject. Individual ISPs made under this MOU will specify the procedure for seeking permission in each case.

**4.3.3** The fee that may be levied by a data controller to comply with a subject access request may be levied and retained by the partner who receives and replies to the request, unless otherwise specified in an individual ISP made under this MOU.

**4.3.4** The partner that receives and replies to a subject access request on behalf of another partner data controller will ensure that the response is sent promptly and before the end of the fortieth day from the date of receipt of the request once all obligations have been met.

**4.3.5** The partner that receives and replies to a subject access request on behalf of another partner data controller will ensure that the request

and response is retained in accordance with the partners policies and procedures in relation to records management.

#### **4.4 Data subjects rights**

**4.4.1** The partners acknowledge that the obligation to respond to a notice to prevent processing under section 10 of the DPA 1998 lies with the data controller.

**4.4.2** A partner that receives a section 10 notice concerning personal data over which that partner and another partner(s) are data controllers will seek the decision of all relevant data controllers before responding to the notice. Receipt of a section 10 notice affecting another data controller will be notified to the relevant partner as soon as practicable after receipt of the notice.

**4.4.3** The partner that receives and replies to a section 10 notice on behalf of another partner data controller will ensure that a written response is provided to the data subject within 21 days from the date of receipt of the notice.

**4.4.4** A decision by a partner to comply with a section 10 notice will be communicated as soon as practicable to any partner processing personal data covered by the notice on behalf of the partner data controller.

**4.4.5** A partner that receives a court order enforcing a section 10 notice will communicate that order to any relevant data controller or data processor partners to ensure that appropriate action is taken.

**4.4.6** A partner that receives a court order to rectify, block, erase or destroy personal data made under section 14 of the DPA 1998 will communicate that order to any relevant data controller or data processor partners to ensure that appropriate action is taken.

#### **4.5 Disclosure to third parties**

**4.5.1** The partners acknowledge that permission to disclose personal data to third parties lies with the data controller.

**4.5.2** A partner that receives a request from a third party for personal data over which that partner and another partner(s) are data controllers will seek the permission of all relevant data controllers before disclosing the personal data. Individual ISPs made under this MOU will specify the procedure for seeking permission in each case.

#### **5.0 PURPOSES FOR WHICH INFORMATION WILL BE SHARED**

**5.0.1** Explicit long term aims for sharing information, identified in conjunction with the Government in 2006 and still valid today, are to provide better

and more joined up care, and advice and assistance to people through the use of computers and communication technologies.

**5.0.2** These arrangements aim to form an efficient and effective business solution to the challenge of sharing personal data in a disciplined, accountable way, allowing front-line staff to deliver improved services to the public.

**5.0.3** The purpose of sharing information at its most pragmatic level, is to work together to collect and share data across the public sector, and to provide the best possible service outcomes for the people of the North East of Scotland.

## **6.0 MANAGING INFORMATION SHARING**

Partners must be satisfied that when sharing information:

- a) The principles contained within Schedule Part A have been adhered to
- b) At least one processing conditions in clause 6.1 has been met and in addition, if sharing sensitive personal data, at least one condition in clause 6.2 has been met.

**6.1** The processing conditions for sharing personal data are:

- The data subject has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the data subject has entered into; or
  - because the data subject has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation applying to the data controller (except an obligation imposed by a contract).
- The processing is necessary to protect the data subject's "vital interests". This condition only applies in cases of life or death.
- The processing is necessary for exercising statutory, governmental, or other public functions or administering justice.
- The processing is in accordance with the "legitimate interests" of the data controller.

**6.2** Processing conditions for sharing sensitive personal data include:

- The data subject who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that there is compliance with employment law.

- The processing is necessary to protect the vital interests of:
  - the data subject (in a case where the data subject's consent cannot be given or reasonably obtained), or
  - another person (in a case where the data subject's consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the data subject consents.
- The data subject has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for exercising statutory, governmental, or other public functions or administering justice.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity and treatment, and is carried out with appropriate safeguards for the rights of data subjects.
- The processing is necessary for the detection of unlawful activity and is in the substantial public interest
- Processing by the police in the exercise of their common law powers

## **6.3 Consent**

**6.3.1** Partners should not rely exclusively on consent to legitimise processing. The Information Commissioner indicates it is better to concentrate on making sure that data subjects are treated fairly rather than on obtaining consent in isolation. Whilst consent is the first in the list of conditions for processing set out in the Act, each condition provides an equally valid basis for processing personal data. It must be noted consent may not be adequate to satisfy the condition for processing and even a valid consent may be withdrawn in some circumstances.

**6.3.2** One of the conditions for processing is that the data subject has consented to their personal data being collected and used in the manner and for the purposes in question.

**6.3.3** Consent is not defined within the Data Protection Act however in Article 2 of the Data Protection Directive it states that consent means

“...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”.

- 6.3.4** The fact that a data subject must “signify” their agreement means that there must be some active communication between the parties. A data subject may “signify” agreement other than in writing; however partners should not infer consent if a data subject does not respond to a communication.
- 6.3.5** Consent must also be appropriate to the age and capacity of the data subject and to the particular circumstances. Consent will not necessarily last forever and it must be recognised that the data subject may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which the information has been collected or used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.
- 6.3.6** Consent should be reviewed to determine appropriateness as a partner’s relationship with a data subject develops, or as their circumstances change.
- 6.3.7** Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
  - the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be “explicit”.
- 6.3.8** A data subject’s explicit consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

## **7.0 DATA QUALITY**

- 7.0.1** An essential requirement of effective information sharing between the partners is data availability and quality. It is the responsibility of each of the partners to ensure that the data held within their systems, whether computer or paper-based, is accurate, up-to-date and relevant. It should be noted that there might be a need for records to contain historical information. It is the responsibility of the partners to ensure

that the quality of the data complies with the duties placed upon them by the Data Protection Act 1998 and other legislation, as well as with the guidance laid down by individual organisations.

## **8.0 ACCESS AND SECURITY PROCEDURES**

### **8.1 Transfer of Personal Data**

**8.1.2** Partners shall ensure that personal data is transferred and shared in a secure manner.

**8.1.3** Where information is shared and processed then the individual ISPs must state in detail the arrangements made for the secure storage, transfer and management of the information. These arrangements must be such that the information is available only to those who have a defined role relative to that purpose. The access privileges of each role must be specified within the ISPs.

### **8.2 Use of Personal Data for Purposes other than those Agreed**

**8.2.1** Where personal data has been shared and processed with partners for a specific purpose, express consent of the data controller must be sought to use the data for another purpose, unless it is in the vital interests of the data subject and consent cannot be easily obtained. Any use of data in this way must be recorded and justified.

### **8.3 Restrictions on the use of statistical and anonymised data**

**8.3.1** Prior to using aggregated statistical data originally collected by another data controller, partners must ensure that data is up to date and fully anonymised so as to render identification of individuals impossible. This will usually involve contacting the Partner who initially produced the information. It is best practice to acknowledge the source of the information in any reports produced.

## **9.0 SECURITY FOR SHARED SYSTEMS**

**9.0.1** Where appropriate responsibility for data archiving, back-up, security and systems integrity of such records shall be agreed between the partners (which may also involve agreement as to sharing any costs associated therewith).

### **9.1 Recording of Individual Data**

**9.1.1** Any of the partners who are involved in integrated teams (being teams comprising the staff of more than one partner/s) shall agree between them, systems for storing personal data.

**9.1.2** If the records of more than one organisation are to be stored by one partner the other partner, whose staff requires access to that information shall ensure that those staff are advised and agree:

- that the information is confidential;
- that access is given to the records purely to enable them to carry out their functions within the joint care team, and is not to be used for any other purpose;
- that the member of staff is only authorised to access records relating to data subjects who have been assigned to that member of staff, and will not access or attempt to access any other records.

**9.1.3** The Partner who holds the records may make it a requirement of granting access that the staff of another Partner first sign confidentiality and conditions of use undertakings.

**9.1.4** In the event of an actual or apparent breach of the confidentiality undertaking referred to above, whichever of the partners employ or employed the individual responsible for the breach or apparent breach shall use its best endeavours to ensure future compliance within the undertaking.

## **10.0 MOU AND ISP MANAGEMENT PROCEDURES**

### **10.1 Formal Approval and Adoption**

**10.1.1** This MOU will be formally endorsed by the Chief Executive of each of the partners.

**10.1.2** This MOU will be formally reviewed six months after its implementation and annually thereafter by the Grampian Data Sharing Partnership, Information Governance Group.

**10.1.3** Individual ISPs will be signed off by the relevant senior personnel dependent upon the context of the Individual Protocol.

**10.1.4** Procedural guidance will be introduced following the development of the partners internal training plans and operational procedures.

## **10.2 Monitoring and Reviewing of ISPs**

**10.2.1** Each individual ISP will set out the particular arrangements for the review of that ISP. These will include details of:

- The partner responsible for reviewing and agreeing changes to the project/service;
- The date of the initial review and the review frequency;
- The partner or individual who will co-ordinate the review.

**10.2.2** In order to monitor adherence to and use of ISPs procedures should be established within each partner for complaints relating to the inappropriate disclosure of information to be reported to each of the other partners.

## **10.3 Resolving issues associated with this MOU and the Individual Protocols**

**10.3.1** Each Partner will be required to log and report any breaches associated with this MOU or any individual ISP. Breaches include any responses and behaviour which the partner reasonably believes is not in accordance with agreed procedures or this MOU.

**10.3.2** All alleged breaches, whether proven or not, should be analysed as part of the formal review process.

**10.3.3** The following types of issues will be analysed:

- Refusal to disclose information;
- Conditions being placed on disclosure;
- Delays in responding to requests;
- Disclosure of information to members of staff who do not have a legitimate reason for access;
- Non-delivery of agreed reports;
- Inappropriate or inadequate use of procedures e.g. insufficient information provided;
- Disregard for procedures;
- The use of personal data for purposes other than those agreed;
- Inadequate security arrangements;
- Any actual or attempted security breach by an external party (eg hacking).

**10.3.4** In dealing with any breach, each Partner will adhere to its own internal and any agreed joint policies and procedures. Any significant or

serious breaches shall be reported to the Grampian Data Sharing Partnership Information Governance Group.

**10.3.5** Individual ISP's will indicate the arrangements made to report and review any breaches associated with this agreed procedure.

## **11.0 AUDIT**

**11.0.1** The partners will keep full details about the personal data shared and the basis on which the information was shared. Accurate records must be kept on disclosed data.

**11.0.2** The operation of this MOU and the individual ISPs and the adherence to the standards identified within each, may be subject to the normal internal and external audit procedures of the partners. Each partner may inform all other partners of its audit programme(s) in relation to ISP's, and will make available the outcome of these audits upon request.

## **12.0 CONTRACTUAL AGREEMENT**

### **12.1 Undertaking**

**12.1.1** The partners accept that the procedures laid down within this document will provide a framework for the sharing of personal data between them in a manner compliant with their legal and professional responsibilities.

### **12.2 Data Protection Notification and Control**

**12.2.1** The partners confirm that each has a valid notification under the DPA 1998 and that this notification includes reference to the fact that personal data held may be disclosed to the other partners.

**12.2.2** The partners undertake not to allow the said notification to lapse or be amended in a way which would render it inconsistent with the clause above for the duration of this MOU.

### **12.3 Duration and Variation**

**12.3.1** This MOU shall come into force immediately upon being executed by all of the partners.

**12.3.2** All new individual ISPs will be developed under the MOU and conform to same.

**12.3.3** The Pan Grampian General Protocols for the Sharing of Information in relation to Children and Young People Services (dated 4<sup>th</sup> September 2008) and Adult Services (dated 3<sup>rd</sup> November 2004) shall remain in force until such time as all existing ISPs made with reference to said Protocols are reviewed to comply with the MOU.

**12.3.4** This MOU shall last indefinitely unless superseded in terms hereof.

**12.3.5** Notwithstanding the termination of this MOU, any duties of confidentiality imposed on the partners or in respect of staff or agents hereunder shall subsist indefinitely.

**12.3.6** Any partner may withdraw from this MOU on giving six months' written notice to the others of their intention to do so.

**12.3.7** This MOU may be varied only by the written agreement of all of the partners.

**12.3.8** This MOU shall terminate on the execution by the partners (or their successors) and coming into force of another Protocol on sharing personal data which is expressly stated to supersede this MOU.

## **12.4 Mutual Indemnities**

**12.4.1** This section shall apply in the event of a breach by any partner, withdrawing from this MOU, of its obligations hereunder (whether or not such breach results in any other partner terminating or purporting to terminate this MOU) where such breach results in harm or distress to any third party.

**12.4.2** In the event that the third party who has suffered harm as a result of such breach seeks damages (whether at common law, under Section 13 of the DPA 1998 or otherwise) from a partner which was not in breach of its obligations, that partner shall be entitled to be indemnified by the partner in breach of its duties hereunder.

**12.4.3** The indemnity referred to above shall include the costs which the partner being indemnified has incurred in resisting or defending the claim for damages.

**12.4.4** The duty to indemnify shall extend to extra judicial settlement of the claim for damages only where the partner in breach has consented to the settlement.

**12.4.5** The duty to indemnify shall include the costs of any appeal against an initial adverse decision of the Court (whether by reclaiming motion or otherwise) but only where the partner in breach has consented to the taking of the appeal.

## **12.5 Alternative Dispute Resolution**

**12.5.1** The partners agree to act in good faith at all times and attempt to resolve any disputes arising as a result of their respective rights and

duties hereunder on an amicable basis. In the event that any of the partners are unable to resolve a specific dispute between/amongst them amicably, the matter shall be referred to a mutually agreed Expert to be determined by the partners.

**12.5.2** Failing agreement, any partner may apply to the Sheriff Principal of Grampian, Highlands and Islands for the appointment of such an Expert. Notwithstanding the method of appointment of the Expert, it shall be an express condition of appointment that any decision shall be issued within 14 days of a statement by all partners involved in the particular dispute, such partners being obliged to act reasonably and expeditiously in the preparation of such statement. Any decision issued by such an Expert shall be binding on all partners except in the event of a manifest error in fact or in law. All partners in the dispute shall bear the costs of appointing the Expert equally or, alternatively, the Expert may, in certain circumstances, determine that one or other partners bears a higher proportion of the costs.

**12.5.3** For the avoidance of doubt, this Section 12.5 shall apply to the duties contained in Section mutual indemnities as it applies to the rest of this MOU.

## **12.6 Definitions**

**12.6.1** In constructing this MOU the expressions contained within Schedule Part B shall have the meanings thereby assigned to them except where the context otherwise requires.

**12.6.2** Except where the context requires, words imparting the singular shall include the plural and words imparting male gender shall include the female (and vice versa).

## **12.7 Governing Law**

This MOU shall be governed by Scots law and the partners who are the parties hereto submit to the exclusive jurisdiction of the Scottish Courts.

We, the undersigned, agree to adopt and adhere to this information sharing MOU **IN WITNESS WHEREOF** these presents typewritten on this and the preceding 17 pages together with the Schedules Part A to D attached hereto are executed as follows:

They are executed for and on behalf of **Aberdeen City Council**, at Aberdeen, by

Signed.....*Alice Watts*.....  
(Authorised Signatory)  
Name **Alice Watts**  
Position **Chief Executive**  
Date **9/5/11**

Signed.....*Sheila Anderson*.....  
(witness)  
Name **SHEILA ANDERSON**  
Position **PERSONAL ASSISTANT**  
Date **9/5/11**

They are sealed with the Common Seal and executed for and on behalf of **Aberdeenshire Council**, at Aberdeen, by

Signed.....*Karen Frances Wiles*.....  
(Authorised Signatory)  
Name **KAREN FRANCES WILES**  
Position **HEAD OF LEGAL & GOVERNANCE**  
Date **11th APRIL 2011**

They are sealed with the Common Seal and executed for and on behalf of **The Moray Council**, at Elgin, by

Signed.....*Alastair Keddie*.....  
(Authorised Signatory)  
Name **ALASTAIR KEDDIE**  
Position **CHIEF EXECUTIVE**  
Date **23 MARCH 2011**

They are executed for and on behalf of **Grampian Health Board** at Aberdeen, by

Signed.....*Richard N. Carey*.....  
(Authorised Signatory)  
Name **RICHARD N. CAREY**  
Position **CHIEF EXECUTIVE**  
Date **24/5/11**

Signed.....*Douglas Cummins*.....  
(Authorised Signatory/Witness)  
Name **DOUGLAS CUMMINGS**  
Position **INFORMATION GOVERNANCE OFFICER**  
Date **24/5/11**

They are executed for and on behalf of **Grampian Police** at Aberdeen, by

Signed.....*Colin McBreacher*.....  
(Authorised Signatory)  
Name **COLIN MCBREACHER**  
Position **CHIEF CONSTABLE**  
Date **27 MAY 2011**

Signed.....*Hary Carr*.....  
(Authorised Signatory/Witness)  
Name **HARY CARR**  
Position **Deputy Director of Grampian Demos**  
Date **21/6/11**

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING MEMORANDUM OF UNDERSTANDING BETWEEN ABERDEEN CITY COUNCIL, NHS GRAMPIAN, ABERDEENSHIRE COUNCIL, THE MORAY COUNCIL AND GRAMPIAN POLICE.

## **SCHEDULE PART A**

### **PRINCIPLES OF THE DATA PROTECTION ACT 1998**

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
  - (a) at least one of the conditions in Schedule 2 is met, and
  - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up-to-date.
5. Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## SCHEDULE PART B

### DICTIONARY OF DEFINITIONS

Applications	Situations in which individual joint working arrangements may be required.
Appropriate Health Professional	shall have the meaning ascribed to it by the Data Protection (Subject to Access Modification)(Health) Order 2000.
Child	A data subject under 16 years of age.
Confidential	As defined in the DPA 1998 and by the Caldicott principles (see also Schedule Part D).
Consent	In this context the authority given by a data subject to an organisation to share information.
Data	Shall have the meaning ascribed to it by the Data Protection Act 1998.
Data Protection Act 1998	The main Act that governs information held on computer and manual records.
Data Protection Principles	The Principles found in Part I of Schedule 1 to the Data Protection Act 1998.
Data Subject	Data subject to whom personal data pertains.
Disclose	The act of passing Individual information to a third party.
Health Board/Authority	A statutory body designated by the Government with executive responsibilities that funds, plans and develops local health services.
Health information	Personal Data to which the Data Protection (Subject Access Modification) (Health) Order 2000 applies.
“Incapable”, “Nearest Relative”, “Primary Carer” and “Welfare Attorney”	shall have the meanings ascribed to them respectively by the Adults with Incapacity Scotland Act 2000, and “Capable” and “Capacity” shall be construed accordingly.
Individual ISP	A Protocol between two or more partners which defines the specific requirements and procedures for data sharing.
Memorandum of Understanding (MOU)	An MOU between two or more partners which defines the general framework and principles for sharing information.
Personal data	shall have the meaning ascribed to it by the Data Protection Act 1998
Processing	shall have the meaning ascribed to it by the Data Protection Act 1998
Procedures	A document describing roles, responsibilities and actions required to achieve a business purpose.
Protocol	In this context, an agreement between organisations which details how they will work together, including how and why they will exchange information.

Secure	As defined in the DPA 1998 and by the Caldicott principles.
Sensitive Personal Data	shall have the meaning ascribed to it by the Data Protection Act 1998
Social work information	means information to which the Data Protection (Subject Access Modification)(Social Work) Order 2000 applies.
Staff	Employees of the partners.
Young person	A data subject aged between 16 and 18 years of age.

## **SCHEDULE PART C**

### **OTHER KEY LEGISLATION**

#### **Introduction**

This Schedule Part summarises the legislation relevant to information sharing. It is provided as a general guide. If you have a need for more detailed guidance this should be sought from your organisation's legal advisors

#### **Access to Health Records Act 1990**

This Act provides rights of access to the health records of deceased data subjects for their personal representatives and others having a claim on the deceased's estate.

#### **Adult Support and Protection (Scotland) Act 2007**

Public bodies must co-operate with each other in dealing with inquiries for assisting in protecting adults from harm

#### **Adults with Incapacity (Scotland) Act 2000**

An Act dealing with arrangements for making decisions on behalf of an adult (16 or over) who lacks capacity to make some or all decisions for themselves. The Act provides mechanisms for authorising people to give consent for an incapable adult.

#### **Age Of Legal Capacity (Scotland) Act 1991**

Once a data subject attains 16 years of age, then that data subject has full legal capacity. For children under 16, then the parent, Guardian or other legal representative can act on the child's behalf unless the child has capacity relating to the particular matter involved. For example, children under 16 have the right to seek information from records concerning them and could likewise have the capacity to provide consent to the disclosure of information concerning them. Whether a child under 16 could consent would depend on whether or not they had sufficient age and maturity to understand the decision being asked of them.

#### **Antisocial Behaviour etc (Scotland) Act 2004**

To effectively manage antisocial behaviour the relevant partners must share information at a local level. Under section 139, any person has the power to release information to a relevant authority where that is necessary for the purposes of any measure in the 2004 Act or any piece of legislation which relates to tackling antisocial behaviour. Clearly this includes exchanging information in relation to ASBO investigations, applications and other relevant matters. The relevant authority means a local authority, a chief constable, the principal reporter, a registered social landlord, and any authority managing Housing Benefit. Section 139 also makes clear that where a person releases information to a relevant authority under this section which is confidential, and they let the authority know about that confidentiality

### **Children (Scotland) Act 1995**

This is the main piece of legislation relevant to the protection of children in Scotland and its main principles are:

- The welfare of the child is the paramount consideration when his or her needs are considered by Courts, Children's hearing and Local Authorities.
- No Court should make an order relating to a child and no Children's Hearing should make a supervision requirement unless the Court or Hearing considers that to do so would be better for the child than making no order or supervision requirement at all.
- The child's views, taking appropriate account of age and understanding, should be taken into account where major decisions are to be made about his or her future.

The Act enables any person to give information to the Reporter if they believe that compulsory measures of care may be necessary to protect a child and requires police and local authorities to do so. It also enables any person to apply to a Sheriff for a Child protection order if they are concerned that the child is suffering or is likely to suffer significant harm.

The child's (anyone under 16) view should be taken into account when decisions are being made about them. A child is presumed to have sufficient age and maturity to express a view at age 12. This means that even if someone is providing consent on behalf of a child, the child's own views should still be sought and taken into account.

### **Crime and Disorder Act 1998**

This Act introduces measures to reduce crime and disorder. This includes the introduction of local crime partnerships around local authority boundaries, to formulate and implement strategies for reducing crime and disorder within the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient for the purposes of the Act. Section 115 does not however impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the data.

### **Criminal Procedure (Scotland) Act 1995**

Sections 52-63 of this Act deal with mentally disordered data subjects, covering matters such as the power of court to commit to hospital an accused suffering from a mental disorder; and the making of interim hospital orders.

### **Disability Discrimination Act 1995**

Imposes a legal obligation on providers of goods, services, facilities and others not to discriminate against those with a disability. It impacts upon matters such as how to deal with subject access requests from those who are unable to write.

### **Education (Scotland) Act 1980**

This Act governs the sharing i.e. disclosure of information by an education authority to parents and children. It does not cover the disclosure of information to other data subjects or partners. Other legislation e.g. Data Protection Act 1998, would therefore apply to such a situation.

### **Freedom of Information (Scotland) Act 2002**

This Act introduced a general statutory right to all types of recorded information of any age held by Scottish Public Authorities.

### **Housing (Scotland) Act 2001**

This Act contains provisions in relation to homelessness, tenancy rights, regulation of the socially rented sector, and the roles and responsibilities of the Scottish Ministers, local authorities, Scottish Homes and other bodies. The 2001 Act builds upon the existing legislative framework, the majority of which dates back to the 1980s.

### **Human Rights Act 1998**

The European Convention of Fundamental Rights and Freedoms 1950 (ECHR) sets out a number of rights and freedoms. The rights and freedoms under the ECHR are given further effect under the this Act

All partners to this MOU are a “*public authority*” within the meaning of the Act and therefore must not act in a manner which is incompatible with ECHR rights. Partners must therefore ensure that their policy making; procedures; exercise of discretion and the decisions which they makes which affect people are compatible with Convention Rights.

Article 8 of the ECHR, provides that “(1) *everyone has the right to respect for his private and family life, his home and his correspondence.*”

(2) *there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*”.

Article 8 should therefore be given due consideration before any action is taken by a public authority which may infringe a data subject’s rights in this respect. In the event of a claim arising under the HRA 1998, that a public authority has acted in a way which is incompatible with the Convention rights (i.e. disclosed their personal data without their consent), a key factor will be

whether the public authority can show, in relation to a particular decision to take a particular course of action:-

Whether it had taken a data subject's rights into account?

Whether the decision taken with respect to those rights was within that organisation's legal powers?

Was the organisation justified in making the decision which it made. A justification to disclose information would be that the disclosure is necessary for public safety; protection of health or morals; prevention of crime or disorder; protection of rights or freedoms of others etc.

apply a "*proportionality test*". The organisation must justify whether the action taken is proportionate to the aim being pursued. The aim pursued should be achieved in a minimalistic way.

Evidence of the undertaking of a proportionality test, weighing the balance on the data subject's right to respect for their privacy against other statutory responsibilities i.e. protection of others from harm etc. will be a significant factor where a partner agency requires to account for its actions, especially where a disclosure is made without a data subject's consent.

### **Management of Offenders etc (Scotland) Act 2005**

This Act states that relevant authorities are to co-operate with one another in the carrying out their functions in relation to a person who is on probation, in custody or subject to the criminal justice social work function of the local authority.

### **Mental Health (Care & Treatment)(Scotland) Act 2003**

This Act covers 4 main areas:-

- it places a range of duties (and gives a range of powers) to organisations involved in mental health law, including mental health service providers, the Mental Welfare Commission, and the Mental Health Tribunal for Scotland;
- It defines clear procedures for decision-making on the compulsory treated and/or detention of people with mental disorder. It sets criteria which have to be met before compulsion can be authorised;
- it amends existing criminal justice legislation to give courts more effective ways of assessing and dealing with a person with mental disorder who comes before them. It defines procedures for the review of orders made by a court in relation to a person with mental disorder;
- it provides a range of new rights for people with mental disorder, such as a right of access to advocacy services; and it provides safeguards on the use of certain medical treatments.

### **Scotland Act 1998**

This Act sets out the jurisdiction and competence of the law making powers of the Scottish Parliament amongst other matters. It provides generally that the Scottish Executive has no power to make any subordinate legislation, or to do any other act, so far as the legislation or act is incompatible with any of the rights under the European Convention on Human Rights or with European

Community law. It also provides judicial remedies for victims of legislation enacted in conflict with the European Convention on Human Rights.

### **The Common Law Duty of Confidentiality**

Scots law recognises a general obligation not to disclose information given in confidence. There is no limit on the type of information which is protected, it is the fact that it is given in confidence which is important.

For the purposes of the common law duty of confidentiality, the duty of confidence only applies to identifiable information which can be linked to a specific data subject. Where personal data cannot be linked to a data subject, then the common law concept of confidentiality will not apply. Unless there is a legal basis to use the information which has been provided in confidence, then the information should only be used for the purposes for which a data subject has been informed, and to which a data subject has given his consent.

The common law duty of confidentiality is not absolute, but can only be overridden by the holder of the information without the consent of the data subject, where it can be justified that the disclosure of such information is within the public interest, for example to protect others from harm; for the prevention or detection of crime etc.

Unless there is a sufficiently robust public interest justification for disclosing identifiable information which has been provided in confidence, then the consent of the data subject should always be sought. Where no consent is gained or forthcoming, then the need for confidentiality would require to be balanced against countervailing public interests

### **Statutory Restrictions on Passing Information**

There are statutory restrictions on passing on certain types of information. The **NHS (Venereal Diseases) Regulations 1974** and **NHS Trusts (Venereal diseases) Regulations 1991** prevent the disclosure of any identifying information about a patient with a venereal disease other than to a medical practitioner under specified circumstances.

**The Human Fertilisation and Embryology Act 1990** (as amended) limits the circumstances in which information may be disclosed by centres licensed under the Act.

**The Abortion regulations 1991** limit and define the circumstances in which information submitted under the Act may be disclosed.

**The Local Government Finance Act 1992** makes it unlawful for Local Authorities to disclose personal data relating to Council Tax to external bodies for non-Council Tax purposes

**The Representation of the People (Scotland) Regulations 2001** makes it a criminal offence for full copies of the electoral register to be disclosed to any other person/body for an unrelated purpose.

**The Enterprise Act 2002** makes it a criminal offence for information relating to individuals and business undertakings which has been gathered as part of Trading Standards investigations under the Act to be disclosed for any other purpose.

### **The Police Act 1997 and The Protection of Children (Scotland) Act 2003**

There are a number of measures to protect children from those who are unsuitable to work with them. One of the measures available is disclosure checks which are used by employers to check the suitability of any prospective employee. The 2003 Act will establish a list of persons who are unsuitable to work with children. The 2003 Act provides that a person working in a child care position (paid or unpaid) will be referred to the List by their employer if he or she harms a child, puts a child at risk of harm and is dismissed, resigns or is moved away from access to children as a consequence.

### **The Protection of Vulnerable Groups (Scotland) Act 2007**

The Act introduces a scheme membership system for people who work with children and protected adults. It will also create, for the first time in Scotland, a list of those who are barred from working with protected adults. If a person is considered unsuitable to work with children, protected adults or both, they will be unable to become a scheme member in relation to either workforce or both.

It will be an offence for an organisation to permit someone who has been barred to undertake such work. The Act permits vetting information to be gathered from police forces and other bodies in order to assess the suitability of scheme applicants and scheme members. This will reduce the number of disclosure forms and checks.

## **SCHEDULE PART D**

### **1.0 CASES OF UNCERTAIN CAPACITY: CHILDREN**

- 1.1 In a case where a professional principally responsible for the care of a data subject who is a child over 12 years of age (hereinafter referred to as the “*relevant professional*”) in exercise of his or her best professional judgement, entertains reasonable doubts as to the capacity of that data subject (which includes a potential data subject) to give consent to the processing of personal data, then, after the relevant professional consults his/her immediate line manager, consent should be sought from a person with the legal authority to act on the child’s behalf i.e. a parent, a guardian in terms of the Children (Scotland) Act 1995 or other person with parental rights.

### **2.0 CASES OF UNCERTAIN CAPACITY: DATA SUBJECT OVER 16**

- 2.1 In a case where a health or social work professional principally responsible for the care of a data subject (hereinafter referred to as the “*relevant professional*”) in exercise of his or her best professional judgement, entertains reasonable doubts as to the capacity of a data subject (which includes a potential data subject) to give consent to the processing of personal data, the data subject’s capacity to give consent requires to be assessed in accordance with the Adults with Incapacity (Scotland) Act 2000:

### **3.0 ASSESSMENT:**

- 3.1 For the purpose of the Adults with Incapacity (Scotland) Act 2000, incapacity must be judged in relation to particular matters, and should not be generalised. Medical practitioners should be alert to this whenever asked to assess capacity for the purposes of the Act. An assessment under the Act should seek to determine whether the adult:

Is capable of making and communicating their choice;  
Understands the nature of what is being asked and why;  
Has memory abilities that allow the retention of information;  
Is aware of any alternatives;  
Has knowledge of the risks and benefits involved;  
Is aware that such information is of personal relevance to them;  
Is aware of their right to refuse, knows how to refuse, and is aware of the consequences of refusal;  
Has ever expressed their wishes relevant to the issue when greater capacity existed;  
Is expressing views consistent with their previously preferred moral, cultural, family and experiential background.

- 3.2 It will also be important to investigate whether any barriers to consent are present i.e. sensory or physical difficulties; undue suggestibility; possible cognitive or physical effects of alcohol, drugs or medication;

possible effects of fatigue; possible effects of pain and mental health status considerations.

#### **4.0 PROCEDURE FOLLOWING ASSESSMENT**

- 4.1 Once an assessment has been completed, the findings of the assessment should be discussed to identify the most appropriate method of communication for that data subject.
- 4.2 The consent should be sought at a meeting/review with a person's relative/s present; their link-worker or key-worker and if appropriate a speech and language therapist.
- 4.3 The data subject's preferred method of communication should be used and any other appropriate verbal or non verbal communication tools to assist the data subject in understanding (i.e. pictorial dialogue, sign language etc).
- 4.4 Every effort should be made to ensure that the data subject is able to understand what is being asked. If the data subject is then able verbally or non-verbally (e.g. thumbs up sign or nod of head) to agree or disagree to consent, then an appropriate consent form should be signed by the data subject and/or their relative and verified by the chairperson of the review.
- 4.5 The information relating to the discussion should be recorded fully in review minutes, stating the method of communication, any tools used to assist and any non verbal forms of communication used. The data subject's responses and those of others present should also be recorded in full. Once completed, the minutes should be read and signed by all present, as this could form part of the recorded consent form.



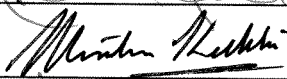

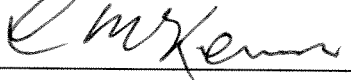
#### **5.0 DETERMINATION THAT DATA SUBJECT IS INCAPABLE OF GIVING CONSENT:**

- 5.1 Where it is determined that a data subject is incapable of giving consent, the relevant professional shall determine whether a Welfare Attorney has been appointed by the data subject (and the document conferring the Power of Attorney duly registered with the Public Guardian in accordance with section 19 of the Adults with Incapacity (Scotland) Act 2000) or whether a guardianship order relating to personal welfare of the data subject (other than one appointing the chief social work officer as guardian) has been made under sections 57 and 58 of that Act, or whether some other person has a legally valid power to consent on the data subject's behalf to matters relating to the data subject's personal welfare.
- 5.2 If any person as described within the paragraph 4.1 above has been appointed and has a duly subsisting authorisation, the relevant

professional shall seek their consent and act on the basis of that consent (or refusal thereof) as if it were that of the data subject.

- 5.3 If no person has been appointed or can be found, the relevant professional shall discuss the situation with the Primary Carer and Nearest Relative of the data subject (if these can be found). Discussions in this respect should specifically include the possibility of making an application under sections 53 and 57 of the Adults with Incapacity (Scotland) Act 2000, to make an Intervention Order or appoint a guardian in relation to the data subject's potential welfare. Thereafter paragraph 4.2 above shall thereafter apply.
- 5.4 If no application is to be made, the relevant professional shall consider the following factors:
- The present and past wishes and feelings of the data subject so far as they can be ascertained by any means of communication, whether human or by mechanical aid (whether of an imperative nature or otherwise) appropriate to the data subject;
  - The views of the Nearest Relative and the Primary Carer of the data subject in so far as it is reasonable and practicable to do so;
  - The views of any guardian, continuing attorney or welfare attorney of the data subject who has powers relating to the proposed intervention; and any person who the sheriff has directed to be consulted, insofar as it is reasonable and practicable to do so; and
  - The views of any person appearing to the relevant professional to have an interest in the welfare of the data subject or in the proposed intervention, where these views have been known to the relevant professional, insofar as it is reasonable and practicable to do so.
- 5.5 If after considering these factors the relevant professional has decided that provision of the services is justifiable in terms of paragraph 4.4, then personal data may be processed by the partners to the extent necessary to provide those services, notwithstanding the lack of consent by the data subject.

Signed

	Aberdeen City Council
	Aberdeenshire Council
	Moray Council
	Grampian Health Board
	Grampian Police

## Document History

**Date of this revision:** FEBRUARY 28<sup>th</sup> 2011  
**Date of Next revision:** Upon signature of all parties, one year from the date of the last signature.

Revision Date	Version	Summary of Changes	Changes Section
September 2007	1.0	First Draft from ACC legal adviser	
September 2008	1.0	Revised Draft Neil Cameron, Grampian Police	
July 2009	1.1	Revised draft, Amanda Roe Aberdeenshire Council	Noted through Track Changes
March 2010	1.3	Revised draft, June Jaffrey Aberdeenshire Council	Noted through Track Changes
May 2010	1.4	Revised draft, Suzanne Davie, Aberdeenshire Council	Noted through Track Changes
June 2010	1.5	Revised draft, Suzanne Davie, Aberdeenshire Council	Noted through Track Changes
August 2010	1.6	Revised draft, Suzanne Davie, Aberdeenshire Council	Noted through track changes
September 2010	1.7	Revised draft, IGG	Noted through track changes
October 2010	1.8	Revised draft, Suzanne Davie, Aberdeenshire Council	Noted through track changes
February 2011	1.9	Final Draft	Final amendments

### Distribution

This document has been distributed to:

Name	Date of Issue	Version
Information Governance Group		1.0
Information Governance Group	27 <sup>th</sup> August 2009	1.1
Information Governance Group	10 <sup>th</sup> May 2010	1.4
Information Governance Group	3 <sup>rd</sup> August 2010	1.6
Information Governance Group	7 <sup>th</sup> September 2010	1.8
GDSP Board	12 <sup>th</sup> November 2010	1.8
Information Governance Group	28 <sup>th</sup> February 2011	1.9
GDSP Board	4 <sup>th</sup> March 2011	1.9

This is a Controlled Document. On receipt of a new version, destroy all previous versions (unless a specified earlier version is in use throughout a Project).