Memorandum of Understanding

for the

Management and Sharing of Information

using the

electronic IRD System

1. Purpose

This memorandum of understanding between City of Edinburgh Council, Lothian and Borders Police and NHS Lothian has been drawn up to describe and agree the governance of the information shared, and decisions recorded, for the protection of children and adults at risk through the electronic IRD system.

2. Background

The three partners regularly share information about a child/adult at risk, and their family, for whom there is a child or adult protection concern, or who has been subject to either a current or historic IRD. To date this has been done in a variety of ways. This has meant that there is no shared memory or means of ensuring that information used for assessment and decision - making is up to date, relevant and accurate. The e-IRD system, via a shared server, has been developed to meet and streamline this process and meet these requirements.

3. Legal Responsibilities

The Chief Executives of the City of Edinburgh Council and of NHS Lothian and the Chief Constable of Lothian and Borders Police are the Data Controllers for the system.

In addition, NHS Lothian undertakes the data processing of all data/information on behalf of the partner organisations and in that will uphold and maintain not only the security of partners' data but also their legal rights and obligations.

Staff in receipt of information from the electronic IRD system should note that information is provided on a child/vulnerable adult for the following purposes:

a) Informing decision-making processes in relation to the welfare of children or adults at risk, as part of an interagency assessment.
b) Investigating suspected crimes against a child or adult at risk
c) Ensuring that the relevant staff directly concerned with the care and protection of

the child or adult at risk have a common and single point in time set of data for each IRD undertaken for that individual.

d) Ensuring that the relevant staff directly concerned with the care and protection of the registered child/adult at risk are in communication with each other so that full participation in Child Protection planning can be assured.
e) Ensuring that there is a shared understanding of decisions made.

4. Roles

The Chief Executives and the Chief Constable will be responsible severally and jointly for the quality, security and use of information held and accessed through the e-IRD system and shared server.

The general governance of information contained on the system, including its security will however, rest with the eIRD board. The Chair of the eIRD Board will be the Senior Information Risk Owner (SIRO) who should ensure that s/he takes advice directly from the Information Governance Working Group; which will report significant risks to the Lothian and Borders Data Sharing Partnership.

The SIRO will refer significant risks and major issues to the eIRD board.

No request for change or change to the system is permitted unless it is agreed by the eIRD Board. The agreement of all or a majority of data controllers is required and all upgrades, programmes for patching, etc, must apply to all partners to ensure the security, robustness and continuing effective application and operation of the system.

5. Responsibilities

All partners will also ensure that:

5.1 Security

The requirements for a system which is classified under the Government Protective Marking Scheme as RESTRICTED (Medical Restricted) are met. This will apply to physical, application and password security and to the transfer and copying of data from the system. The confidentiality of certain data contained in the system must be recognised and dealt with accordingly as should the higher level of protection required to prevent unauthorised mass extraction of personal data.

5.2 Vetting

All partners will ensure that all users or administrators of the system are vetted to the level appropriate to their role and access rights.

5.3 Training and Access

Each partner will be responsible for ensuring that all operators and users of the system are trained to the required level (Access, Manager, Administrator, Local Controller); and

agree to adhere to the controls laid down in the Operating Procedure and Protocol

No 'user' will be permitted access to the system until they have undergone the agreed training; and access rights will be set by the local controller with responsibility for Identity Access Management. That information will be forwarded to the Administrator who is responsible for the day to day administration of the system.

Partners are responsible for ensuring that all local access rights are kept up to date and that access (or level of access) is removed from users when roles change. Access rights will be subject to audit.

Training will include the importance of secure and appropriate access and use of the system; including the importance of data accuracy, quality and review and of password protection. The application of relevant business rules will also be covered.

5.4 Data Quality

Data quality, and the retention and review of information will be governed by the relevant policies and business rules with which all partners will comply. Any change to the business rules will be decided on and agreed by the eIRD Board.

All partners will be responsible for ensuring that the business processes and rules for data quality are followed.

Relevant local data quality issues will also be reported to the eIRD Board. Even where local issues are identified, and local solutions found, reports should be made to the eIRD Board so that lessons can be learnt, shared and training reviewed.

All partners must ensure that only relevant and appropriate information is entered on to or transferred into the system.

5.5 Audit

Each partner will be responsible for ensuring that access to and use of all data from the e-IRD system is only for the stated purpose of sharing under and ensuring the management of the IRD process.

Questions about audit and the use of information will be referred to the eIRD board.

5.6 Research

All requests to use data from the e-IRD system for research projects will be referred to the eIRD Board. Advice on the research proposal, and access to, the use of, and the security of data, must be sought from the appointed representatives of the Data Controllers.

6. Breaches of Security

All known or suspected breaches of security in relation to the system, terminals and /or

any information - such as misuse or abuse of the system, misuse or abuse of protocol information, unauthorised processing of data, unauthorised disclosure of information, malicious software attack, denial of service attack - are to be reported to the respective organisations' Information Security Officer, Data Protection Officer or equivalent. Once notified of a breach of security an investigation will take place to identify, where possible, who carried out the breach, what information has been compromised, whether the integrity of the system has been compromised etc.

Where any breach of security may amount to criminal activity, this must be reported to Lothian and Borders Police which will investigate the matter and, where appropriate, report the circumstances to the Procurator Fiscal.

Where relevant or necessary, all partners are to be informed of any breach and provided with sufficient details which will enable them to retain assurance in the confidentiality, integrity and availability of the information and the processes supporting information exchange, and to undertake their own risk assessments.

7. Access to Information

Access to information gathered as part of any of these processes is available either under subject access rights, as described in the Data Protection Act 1998 (Section 7), or the Freedom of Information (Scotland) Act 2002 (FOI). Where access is requested advice must be sought from the organisation's Freedom of Information or Data Officer.

Where a request has been received and a partner holds any information that originated from another partner or where a partner is considering the disclosure of information that may impact on another partner, then it is recommended that the originator of the information is consulted prior to any disclosure. The ultimate decision as to whether to disclose the information lies with the organisation that received the request; however, the originator of the information should be given the opportunity to ensure that FOI (or Data Protection) exemptions are suitably applied.

Complaints from data subjects, or their representatives, about information held by the partnership will be investigated first by the partner receiving the complaint, although action that affects any of the signatories will not be taken without the consent of all relevant parties.

8. Liability

The onus will be on each Partner to this Memorandum of Understanding to ensure that Confidential and Sensitive information is protected from unauthorised disclosure.

(Sensitive information is defined in Schedule 3 of the Data Protection Act 1998).

9. Review

This protocol will be reviewed annually or sooner if material changes are required.

Signed on behalf of

Name
Position

Date

Signature ……
City of Edinburgh Council

Name
Position

Date

Signature ……..
Lothian and Borders Police

Name
Position

Date

Signature ……
NHS Lothian