

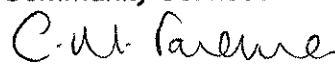
This is an internal Data Exchange Agreement between council services to be used in conjunction with council policies and government legislation

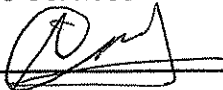
Services involved


Isle of Wight Council

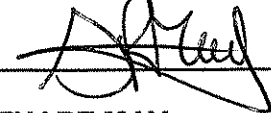
- Community Services
- Childrens Services
- Customer Services (Caldicott Guardian)
- Fire & Rescue Services

Signatories

Service: Community Services
Signed: 
Name: CLAIR FOREMAN
Date: 23.6.08

Service: Childrens Services
Signed: 
Name: NICOLAS CRICK
Date: 24/6/08

Service: Customer Services
Signed: 
Name: MARCUS ELSOM (Caldicott Guardian)
Date: 30/6/8

Service: Fire & Rescue Services
Signed: 
Name: STUART MAY
Date: 24/06/08

1. Purpose of this Data Exchange Agreement

This Data Exchange Agreement (DEA) is for the purpose of exchanging information between the signatory services listed above. The information will be used for the purposes of the protection of vulnerable adults and children within the Isle of Wight Council between Social Care Services (Community Services and Childrens Services) and Fire & Rescue Services.

2. Legal Basis of this agreement

This agreement involves partner services within the Isle of Wight Council and therefore the council's own Data Protection Act registration applies, and ensures that there is a legal basis for the sharing of the agreed information.

This agreement is also based on the provisions as set out in the Civil Contingencies Act and associated guidance, which provide the Isle of Wight Council with the authority and legal basis to implement this agreement with regard to emergency response.

The Government's Caldicott Regulations also apply. The Guardian is responsible for the establishment of procedures governing access to and the use of personally identifiable information within the Isle of Wight Council, and where local flexibilities exist, the transfer of such information from the organisation to other bodies. In agreeing local procedures and policies, the Guardian should ensure consistency with any relevant central requirements and guidance.

2.1 Extent and type of information to be shared

The Isle of Wight Council will ensure that the current annual consent review includes notification of this use of their data is included and explained to Service Users.

3. Agreed Information Datasets and Frequency of Reports

3.1 Report

Report Name: Emergency Response Report

- Address
- Contact Number
- Vulnerability/Client Category
- Known Hazards
- Carer name and contact details
- Language details

3.2 Frequency

The report for emergency response purposes will run nightly and downloaded daily to the Fire Service's WINGS system, which will only be accessed on the explicit approval of the Caldicott Guardian or their delegated officer in the case of an emergency.

3.3 Approval for Access and Release

The Fire Control Centre will telephone either of the following officers to obtain consent for the access and release of the agreed information to the authorised emergency response officer in charge.

Caldicott Guardian: Marcus Elsom on 07807159533

Caldicott Co-ordinator: Susanne Holman-Harris on 07779999825

3.4 Method of Communication

The report will be run nightly via Business Object XI, which will be stored securely on a central share drive that can be accessed by the relevant officers on the approval of the Caldicott Guardian.

4. Responsibility

The Performance & Information Team will develop and schedule the report.

5. Retention

The information will be run nightly with the dataset will be overwritten and the information will be stored on a secure network drive with authorised access only with Caldicott Guardian approval to access and release only.

6. Constraints

This agreement must operate within the constraints of the purposes as listed within this document in order for the law sharing of this information to exist.

7. Feedback

7.1 Agreed Feedback Format

Review Meetings to review the reports provided and feedback questionnaires as appropriate

7.2 Frequency of Feedback

Initially monthly and then bi-monthly as necessary

8. How this information may be used

The information may only be used by the person requesting it to assist the management of Emergency Response for the protection of vulnerable adults and children.

9. Security and Data Management

The security of the information disclosed is the responsibility of the partner service requesting the information and it must not be copied or transferred into any other medium or disclosed to anyone not listed in the agreement or outside the remit of the agreement.

The designated employees of the partner services who will have access to the information will abide by the security and data management restrictions as stated in the Council's Information Disclosure document.

10. Storage of Information

The information for emergency response purposes will need to be stored on an encrypted laptop with the information removed once the purpose of the use of this information has been concluded. The laptop when not in use will need to be stored securely within a safe haven location. Authorised access with password protection will be required.

11. Complaints and Breaches of Confidentiality

The partner organisation providing the information is responsible for any complaints or appeals process. Any Data Protection or Freedom of Information requests must be responded to only after consultation with the partner organisation which provided the information.

The Principal Designated Officer for each agency must be notified immediately of any of the above. All complaints must be acknowledged in writing within 2 days and, wherever possible, dealt with within 28 days. Any disciplinary proceedings will be implemented according to the Isle of Wight Council's policies.

12. Data Quality

Please note at the signing of this agreement the quality of the data is currently being reviewed and as such the data quality cannot be completely assured as 100% accurate, and therefore must be used with caution as legislation may possibly be breached and an individual's rights infringed under such circumstances.

13. General Operational Guidance

13.1 Audit

PDO's and PO's must be mindful of the use they make of information specified within this agreement and whether their decision will stand scrutiny at a later stage. This should not, however, be a barrier to the disclosure of information in appropriate circumstances, but will necessitate the keeping of adequate records of disclosure and the reasons for them.

It is the responsibility of the Designated Officers of the partner services to review this agreement annually and it is the responsibility of all the Principal Designated Officers, listed below, to ensure that information is being used and stored in the correct manner and that the list of Designated Officers is up to date.

13.2 Closure or termination of agreement

Any partner service may suspend this agreement if they feel that security has been seriously breached.

This agreement may be terminated if there is a serious breach of confidentiality for example, where information provided under the agreement is used for purposes other than set out in this agreement or information is passed to a third party other than with the agreement of the provider.

14. Designated Officers

Each service must appoint a Principal Designated Officer (PDO) who is a manager of sufficient standing and has a coordinating and authorising role. It is recommended that a Designated Officer (DO) is also appointed within each partner service the details of whom are listed below.

The named individuals listed are designated to assume responsibility for data protection, security and confidentiality and compliance with all relevant legislation. Specific responsibilities of the PDO and DO are as follows but not limited to:

- Ensuring that all sections of this agreement are adhered to.
- Ensuring that all PDO's, DO's and other staff are fully aware of their responsibilities.
- Ensuring the agreement is accurate, up to date and adequate for the purpose for which it is intended.

Department	DEA Role	Position	Telephone No.	Secure Fax No.
Customer Services	Principal Designated Officer	Marcus Elsom Head of Modernisation	01983 823099 ext. 6509	
Customer Services	Designated Officer	Susanne Holman-Harris Information Governance Manager	01983 823099 ext. 6566	
Fire & Rescue Services	Principal Designated Officer	Stuart May Group Manager, Prevention, Protection and Response	01983 823099 Ext. 8188	
Fire & Rescue Services	Designated Officer			

15. Review of this agreement

This agreement will be subject to a formal annual review. All breaches of the policy are to be logged, investigated and the outcome noted and acted upon.

16. Future Development of Information Sharing

Any future development of the type and scope of the information formally shared by partner agencies will require further discussion and formal agreement by the relevant Senior Management Team and Cabinet Members.