

Schedule 2

Information Sharing Protocol for the Devon Learning Disability Partnership Employee Access to Devon County Council Computer Systems and Information

1. Purpose

The purpose of this Protocol is to enable the sharing of information consistent with requirements detailed in "Information for Health", "Information for Social Care", the service user-based National Service Frameworks white papers produced by the Department of Health, "Care Direct" and "Supporting People".

This Protocol is aimed at the following partner organisations:-

Devon County Council (DCC)
Devon Primary Care Trust
Acute Trusts (Royal Devon & Exeter Hospital and North Devon District Hospital)
Devon District Councils
Devon Partnership NHS Trust (DPT)
Torbay Care Trust

This Schedule forms part of the Agreement signed by Devon County Council and the Devon Partnership NHS Trust and is concerned with allowing Assigned Employees from the Trust to have access to:-

- Devon County Council Social Care Management System (CareFirst) and manual records that contain personal data relating to Social Care service users and Devon County Council employees.
- Microsoft Outlook System (includes Devon County Council employee email addresses and calendar information).
- Appropriate network folders.
- Stand-alone computer systems containing service user information as appropriate.
- Use of the Internet.
- Use of the Intranet.

(Note: The above list needs to be consistent with clause 2.1 of the main Agreement)

It will be the responsibility of the parties to ensure that:-

- Ethical standards are maintained.
- Appropriate training and awareness is provided.
- Adequate arrangements exist to test adherence to the Protocol.

2. Introduction

This Protocol has been developed as an operational Protocol under the terms of the overarching Devon Health and Social Care Organisations Protocol for sharing Person-Identifiable Information between Organisations. It should be read in conjunction with this overarching Protocol.

The parties subscribe to the following for this Protocol:-

- The Data Protection principles must be upheld.
- This Protocol must be reviewed regularly.
- The Trust may request any change to the Protocol at any time by submitting to Devon County Council a suggested revision.
- The nominated holder of this Protocol is Tim Golby, Assistant Director Finance and Business Support, Devon County Council Adult & Community Services (ACS) and Caldicott Guardian, who shall ensure that the Agreement and Protocol are kept under regular review on an annual basis or as necessary.

3. Standards

3.1 Purposes for which Information may be used and shared

Access will be given to the Social Care system(s), Outlook, network folders and manual records to enable Assigned Employees from the Trust to carry out their work and statutory functions, thus enabling joint working and effective communication. [Note: This ties in with list in the Agreement]

Devon County Council Social Care staff will have access to Health patient information input to the Care Management system CareFirst, to enable them to carry out their statutory functions under joint working conditions.

Information obtained from the Council's computer systems and manual records must not be used or disclosed for any other incompatible purpose(s).

3.2 Security and Access to CareFirst

System security access to CareFirst has been established for all Learning Disability Partnership users based on their job roles and responsibilities. This is set out in a separate paper "Phase 5 Electronic Social Care Record (Learning Disability Service) Security and Access".

3.3 Compliance with Devon County Council's Corporate Policies

Assigned Employees from the Trust must comply with Devon County Council's corporate policies and Codes of Practice relating to use of the computer systems and information and the Joint Partnership Security Policy. Copies of all relevant documents and Policies will be made available to them.

3.4 Audit and Compliance Monitoring

Devon County Council reserves the right to monitor routinely use of the Social Care System, email and the intranet and to audit activity and access to its systems. An audit trail is maintained for the Social Care System and staff access should be on a strict need to know basis; any breach may result in disciplinary action.

Audit activity includes the right to visit relevant offices. Assigned Employees will be expected to co-operate and provide relevant information on request, even if though they are not employed directly by the Council.

3.5 Sharing of Information

Devon County Council employees have been informed that their email addresses, calendar information and information held in network folders will be shared with the Trust for multi-agency purposes only.

Service user personal information should normally only be shared between partner agencies with the explicit and informed consent of the individual (or their representative) concerned, except in exceptional circumstances e.g. where sharing is necessary to safeguard public safety or in an emergency situation. Consent is recorded on the SAP6 “Consent to Share and Protect your Personal Information” form.

Where relevant to the work of the Trust and taking into consideration any duties of confidentiality to Devon County Council employees, relevant information may be disclosed to third parties on a strict need to know basis only.

Disclosures of information from the Social Care system(s) and manual records must not be disclosed to external organisations not listed in this Protocol, unless the service user’s consent has been obtained or it has been authorised by the Caldicott Guardian or Senior Information Governance Officer (ACS) (see Appendix D for contact information). If in any doubt about whether or not to disclose information, partner employees should seek advice from this person.

Disclosures can also take place under certain circumstances, where there is an exemption under the Data Protection Act. This is unlikely to arise under the working arrangements envisaged under this Protocol, but if they do, they must be assessed on a case by case basis and authorised by the Caldicott Guardian or Senior Information Governance Officer (ACS). (See Appendix E for a list of non-disclosure exemptions).

3.6 Confidentiality

Both Trust and DCC employees shall at all times comply with any duty of confidentiality towards individuals whose personal data is supplied or made available under this Protocol. This requirement shall survive termination of the Agreement and Protocol or the removal of any individual assigned employee from employment.

The Caldicott principles must be upheld in relation to all personal information. See Appendix C.

3.7 Recording and Storing Information on the Social Care System (CareFirst)

It is important and necessary to record information on CareFirst that needs to be shared in order to provide safe care and where missing information could be dangerous if it doesn’t give the complete picture.

Information to be recorded includes:

- demographic details such as name, address, telephone number, gender, date of birth, carer details (if applicable) and ethnicity.
- standard personal health and social care case recording information, advice, details of visits and any services in place.
- staff contact details.

Information is recorded on relevant forms and is then available to Partnership staff in any location to view in a standardised recording format. (See Appendix A for a list of forms to be completed electronically on CareFirst).

There may be **exceptional** circumstances where particular confidential information should not be shared and therefore not recorded on CareFirst. In these circumstances a note can be made on the electronic record to indicate there is additional manual information available held securely elsewhere, with the location and name of contact person.

Circumstances where information may not be recorded on CareFirst:

- sensitive health/medical information that may make up part of a specialist assessment (e.g. HIV status/drug use). If the information is not to be shared the risk to the individual of not sharing the information should be assessed.
- information which would not normally be shared with other team members or that has been provided by an individual in confidence on the understanding it will not be shared (e.g. involving a staff member who is also a service user or carer).
- where the person or someone acting on their behalf has specifically prohibited the sharing of their information. In these circumstances the person should be informed that if we are unable to share their information we will not be able to provide co-ordinated services and it may mean a reduction in services to them.

3.8 Lawful use

Use of Devon County Council's information systems must be lawful, and comply with relevant law, such as, but not limited to the Common Law Duty of Confidentiality, Computer Misuse Act 1990, the Data Protection Act 1998 and any laws relating to defamation.

3.9 Accuracy, relevance and adequacy of information

Each employee has a responsibility to ensure that both Health and Social Care information stored on the DCC Social Care system(s) is adequate, relevant, kept up to date, accurate and is not excessive for the purpose of processing it.

3.10 Retention of information

Information must not be held for longer than necessary. It follows that information must be deleted as soon as it is no longer required for the original purpose for which it was supplied or collected under confidential conditions such as shredding.

There are minimum national guidelines for all types of health records published by the Department of Health contained in the "Records Management: NHS Code of Practice". Where joint records exist containing both Health and Social Care records the longer of the two retention periods should be adopted.

Partnership employees should be aware of Devon Social Care policy on retention of information entitled "Record Handling, Management and Retention", available separately, to include retention periods for joint records based on the guidelines above.

3.11 Security

Assigned Employees must take all reasonable steps to ensure that they comply with any appropriate technical and organisational measures which are in place (a joint Partnership Security Policy is available separately), to protect any personal data accessed or processed by Partner employees against:-

- Unauthorised or unlawful processing of personal data.
- Its accidental loss.
- Destruction or damage.

This includes paper files where information from the Outlook system and network folders may be recorded.

Passwords must be kept secure and must not be shared with third parties or other partner organisation team members.

Highly confidential or sensitive information must not be sent by e-mail to external recipients via the Internet unless it has been encrypted, because the Internet is not completely secure.

Documents sent as attachments must be password protected. This will encrypt the attachment (for the purpose of this Protocol guidelines) rendering the document useless without it.

Email sent internally between staff on the DCC network, is considered secure and encryption is not required.

Assigned Employees should be aware that, unless a meeting is marked as “private”, information they record in the Outlook Calendar system is visible to all Devon County Council staff and Partnership Organisations with access to the DCC network.

On leaving the Partnership, Associated Employees must not take with them any personal data governed by this Protocol. It must be securely destroyed or returned to Devon County Council.

3.12 Training

Assigned Employees must be appropriately trained in the use of Devon County Council computer systems, and be informed of their responsibilities for confidentiality and Data Protection Act compliance.

3.13 Subject Access Requests

Where joint records are held between Health and Social Care, such as in the Learning Disability Multi-Disciplinary Team, the person who wishes to access their records can apply to either organisation who can provide access to the joint record, provided that the data subject (the individual who is the subject of the personal data or information) is informed that the data are held jointly.

There are procedures in place both within Devon County Council and the Devon Partnership Trust to ensure that the data subject is able to access their records without having to apply to each partner for access and to inform each other that access has been given.

It is the policy of Devon County Council not to charge for access to social care records. If the request includes medical records the Devon Partnership Trust may make a charge to cover costs of the copying as is their entitlement under the Data Protection Act.

3.14 Complaints

Any complaint received about misuse or abuse of the IT systems made will be brought to the attention of the nominated officer of the relevant partner organisation who will be asked to deal with the matter accordingly.

Appendix A

Forms to be held and completed electronically on CareFirst

- Background and Contact Assessment
- Overview Assessment
- Consent to Share and Protect your Personal Information
- FACS Eligibility Checklist
- Care Plan
- Review
- SAP Health Needs Assessment (HNA)

- Core Assessment LD
- Entitlement
- RAS
- RAS Level
- Transfer Information
- Health Assessment Summary
- Health Intervention Outcomes
- Needs and Outcomes

For future input on CareFirst

- Personal Risk Assessment (DPT)
- Panel Application

Appendix B

Definitions

“**Personal data**” is information that relates to a living individual that can be identified from those data or from those data and other information which is in the possession of or is likely to come into the possession of the data controller. It includes any expression of opinion or intentions in respect of the individual.

“**Processing**” of personal data means obtaining, recording or holding the information or data, or carrying out any operation, including:-

- Organisation, adaptation or alteration.
- Retrieval, consultation or use.
- Disclosure by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.

Appendix C

The Caldicott Principles

- **Principle 1 – Justify the purpose(s)**

Every proposed use or transfer of person-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

- **Principle 2 – Don't use person-identifiable information unless it is absolutely necessary**

Person-identifiable information items should not be used unless there is no alternative.

- **Principle 3 – Use the minimum necessary person-identifiable information**

Where use of person-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.

- **Principle 4 – Access to person-identifiable information should be on a strict need to know basis**

Only those individuals who need access to person-identifiable information should have access to it, and they should only have access to the information items that they need to see.

- **Principle 5 – Everyone should be aware of their responsibilities**

Action should be taken to ensure that those handling person-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect a person's confidentiality.

- **Principle 6 – Understand and comply with the law**

Every use of person-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Appendix D

Contact Information

For further information or any queries to do with this Protocol please contact:

Caroline Hitchcock
Senior Information Governance Officer (ACS)
Social Care Information Systems Team
County Hall,
The Annexe
Topsham Road,
Exeter,
EX2 4QR

Telephone: 01392 384395

Email: caroline.hitchcock@devon.gov.uk

Appendix E

Circumstances when information may be disclosed – non-disclosure exemptions

Disclosures can take place under certain circumstances under the Act's non-disclosure provisions. Reliance on these must be assessed on a case by case basis. The provisions that would apply are:-

- At the request of and with the consent of the individual concerned, or someone acting on their behalf.
- For the prevention or detection of crime, the apprehension or prosecution of offenders, and taxation purposes. Request for information must be on a case by case basis and where failure to provide the information would seriously prejudice these purposes. All requests and responses must be appropriately authorised and documented.
- Where information is made available to the public by or under enactment.
- Where the disclosure is required by law or by the order of a court.
- Where the disclosure is made in connection with legal proceedings, for the purpose of obtaining legal advice, and establishing, exercising or defending legal rights.
- For the purpose of safeguarding national security.
- By order of the Secretary of State.
- Regulatory Activity – applies to numerous different categories of regulatory function exercised by public “watch-dogs” which are all variously concerned with the protection of members of the public, charities or fair competition in business. This is not a blanket exemption and is only available to the extent that the application of any or all of such provisions would be likely to prejudice the proper discharge of those functions.
- Special purposes – the special purposes means any one or more of:-
 - a) journalism,
 - b) artistic purposes,
 - c) literary purposes.
- Research, History and Statistics – The Act provides for various exemptions in respect of the processing (or further processing) of personal data for research purposes (including statistical or historical purposes) provided that the processing (or further processing) is exclusively for those purposes and, also, that the following conditions are met:-

That the data are not processed to support measures or decisions relating to particular individuals, and

That the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

- Domestic Purposes – this is a wide-ranging exemption whereby personal data are exempt from the Data Protection Principles and the provisions of Part II (individual rights) and Part III (notification) of the Act. It applies where they are processed by an individual only for the purposes of their personal, family or household affairs (including recreational purposes).

January 2008