



LINCOLNSHIRE & RUTLAND

**EVALUATION OF THE
LINCOLNSHIRE CONNEXIONS PILOT**

REPORT 1: POOLING AND TRACKING

Bill Cooper

&

Anne McCann

CeGS
Centre for
Guidance Studies

April 2001

CONTENTS

	<u>Page</u>
Preface	1
Executive Summary	2
Introduction	3
Methodology	4-5
Findings	5-6
Key Lessons	7
Recommendations	7
Appendices	
Appendix 1 Data Sharing Protocol (Draft)	
Appendix 2 Technical sub group report	
Appendix 3 Draft Client Consent Form	

PREFACE

We are greatly indebted to the following team members for their contributions and support throughout the project: David Clark, Lincolnshire Social Services; Trevor Cockburn, Lincolnshire Youth Service; Chris Garrett, Lincolnshire Social Services Young Persons Substance Misuse Information Officer; Linda Graham, Lincolnshire Careers and Guidance Services, Clive Hadfield, Rutland County Council; Keith Henton, Lincolnshire Social Services; Colin Knowles, Lincolnshire Police; Rachel Markham, Lincolnshire Health Authority; Alan Pankhurst, Lincolnshire Development; Garry Peppard, Youth Offending Team; Tracey Robinson, Lincolnshire County Council Education Welfare Service; Pat Taylor, Leicestershire Careers; Paul Tunmore, Lincolnshire County Council and Bernie Wiltowski, Lincolnshire Training and Enterprise Council Secondment Project.

We also wish to thank all the young people and other professionals who helped us during our research.

Bill Cooper & Anne McCann
Pilot Project 1

EXECUTIVE SUMMARY

This report examines our attempts to promote and put in place arrangements across all main Connexions partners in Lincolnshire and Rutland to enable the sharing of data on young people. We have tried to draw out what we now think will work and why, what problems we met, and what (if anything) we would have approached differently.

Section 1 outlines the project development plan and the original approach which was to first test the feasibility of sharing information by linking databases, within an agreed protocol; and then to actually pilot linked databases. We have included here the change to this approach necessitated when the mapping of databases across partners was completed. This showed only one current and broad database dealing specifically with young people, the Lincolnshire Careers Service database known as Aspire.

Section 2 examines the reasons for choosing a two-phase approach to the project, the main one being the structure of the project funding. A portion of this funding was withheld because of proposed national developments. We earmarked this part of the funding for piloting the linkage of three existing databases and ultimately used it for capacity building within Connexions partners. However nationally the picture did evolve and the potential for a national database is being explored. Our pilot will complement this work by informing DfEE early in the process about issues that were common to all partners, and particularly clarifying the legal framework within which partnerships have to operate. Our approach was to use a multi-agency team to develop protocols, establish the current position and advise on underpinning practice, for example client consent and practitioner training and management.

Section 3 looks in more depth at the process throughout the project, particularly turning points in terms of understanding and also the technical issues that we met. Within the tight time-scales the aim was to keep the project at a practical level, try out practices and develop processes. We have had an indication from DfEE that the protocol for data sharing and the client consent form developed from the pilot is capable of use by other Connexions partnerships.

Section 4 reviews the key lessons learned. This project highlighted the differences between cultures that will be working together within Connexions partnerships. We realised that if practitioners found the formal process of data sharing too cumbersome they would actually avoid it. This might not disadvantage the individual young people, where informal data sharing practices are already used, but would hamper service development and in that way ultimately all clients. There are real issues about the legal structure within which personal information can be used. Another major lesson was to recognise the difference between common data to identify individuals and sharing information on these individuals

Section 5 presents the conclusions from the project and provides a set of recommendations to inform the future development of the Connexions Services at a local and national level.

1. INTRODUCTION

- 1.1 This report examines our attempts to promote and put in place arrangements across all main Connexions partners in Lincolnshire and Rutland to enable the sharing of data on young people. The overall aim of the project being to 'increase our understanding of the status and experiences of young people by gathering, sharing and analysing client data in the most cost effective way'. We have tried to draw out what we now think will work and why, what problems we met and what if anything we would have approached differently.
- 1.2 The concept of understanding and recording the status of young people at all stages between the ages of 13 and 19 is not a new one. Personal data is shared regularly within professions and across professions dealing with young people. However the world is changing, young people are aware of their 'rights' and they have more of them than ever before, particularly in the area of personal information.
- 1.3 It was important to create an arena of safety within which Connexions partners share and accurately represent the status of young people. This involved an approach encompassing both technical and cultural solutions.
- 1.4 The aim of the project was to:

'Increase our understanding of the status and experiences of young people by gathering, sharing and analysing client data in the most cost effective way.'
(Pilot Project Development Plan, 2000)

Project milestones:

- Multi-agency project team established
- Map data sources*
- Multi-agency commitment to share data
- Multi-agency data pooling protocols completed
- Report on potential for client database linkages
- Link at least three client databases
- Recommendations for extended database linking/single client database
- Monitor and evaluate process

*When we completed the initial database mapping it became obvious that organisations within the Connexions partnership had differing levels of technical capability and it was therefore unlikely that any databases could be linked. However an agreement was reached that allowed a way forward using one database and developing partner access to this database. (See Table 1).

- 1.5 In reality this quite neatly dealt with some of the thorny issues about data integrity and also provided the partnership with an advanced set of data.

2. METHODOLOGY

- 2.1 Following a joint conference on confidentiality issues organised by Pilot 6 – The Unification of Diagnostic Tools project. The multi-agency team was put together (with a link to Pilot 6). The main aim was to ensure representation from the major partners and organisations within Connexions.
- 2.2 A decision to hold back some of the project funding by DfEE because of proposed national developments made it sensible to split the pilot into two parts. The first part involved actually preparing the ground and making a case for the release of further funding to pilot linking of databases in Lincolnshire Connexions.
- 2.3 In the event, the first part of the project shone a light on the obvious potential of using the Lincolnshire Careers Service database - Aspire. We could then concentrate the technical effort on exploring ways of allowing partner organisations access to Aspire.

Table 1: Data currently held electronically by partner organisations

	Organisation (Key to abbreviations – see page 3)								
Data Held	LCC	RCC	EWS	SSD	YOT	POL	YS	LCGS	LTEC
Name	Some	Yes	Yes	Yes	Yes	Yes	Some	Yes	Yes
Address	Some	Yes	Yes	Yes	Yes	Yes	Some	Yes	Yes
DoB.	Some	Yes?	Yes	Yes	Yes	Yes	Some	Yes	Yes
Gender	Some			Yes				Yes	Yes
Ethnicity	Some			Yes	Yes		Some	Yes	Yes
Disability	Some			Yes			Some	Yes	Yes
School	Some	Yes	Yes	Some	Yes		Some	Yes	
College					Yes		Some	Yes	Yes
Workplace					Yes		Some	Yes	
Age	3 - 19	4 – 16	5 - 16	0 - 100	10 – 17	0 - 100	11 – 25	13 - 25	16 - 25
Cohort Size	100,000	4,500	5,000	70,000	532	Unknown	Unknown	54,000	4,500
Cohort Size 13-20				4,000	532	Unknown	Unknown	54,000	3,500
CSV Export	Yes	Yes???	No???	Yes	Yes???	No	No	Yes	Yes
Internet Access	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes

Lincolnshire County Council (LCC) is at the moment developing a new student database that is not planned to be fully functional until February 2002. This means that in the short-term there is no single definitive listing of school pupil data other than that held by LC&GS.

The Youth Service (YS) tend to collect data in paper format, although some stand- alone databases do exist.

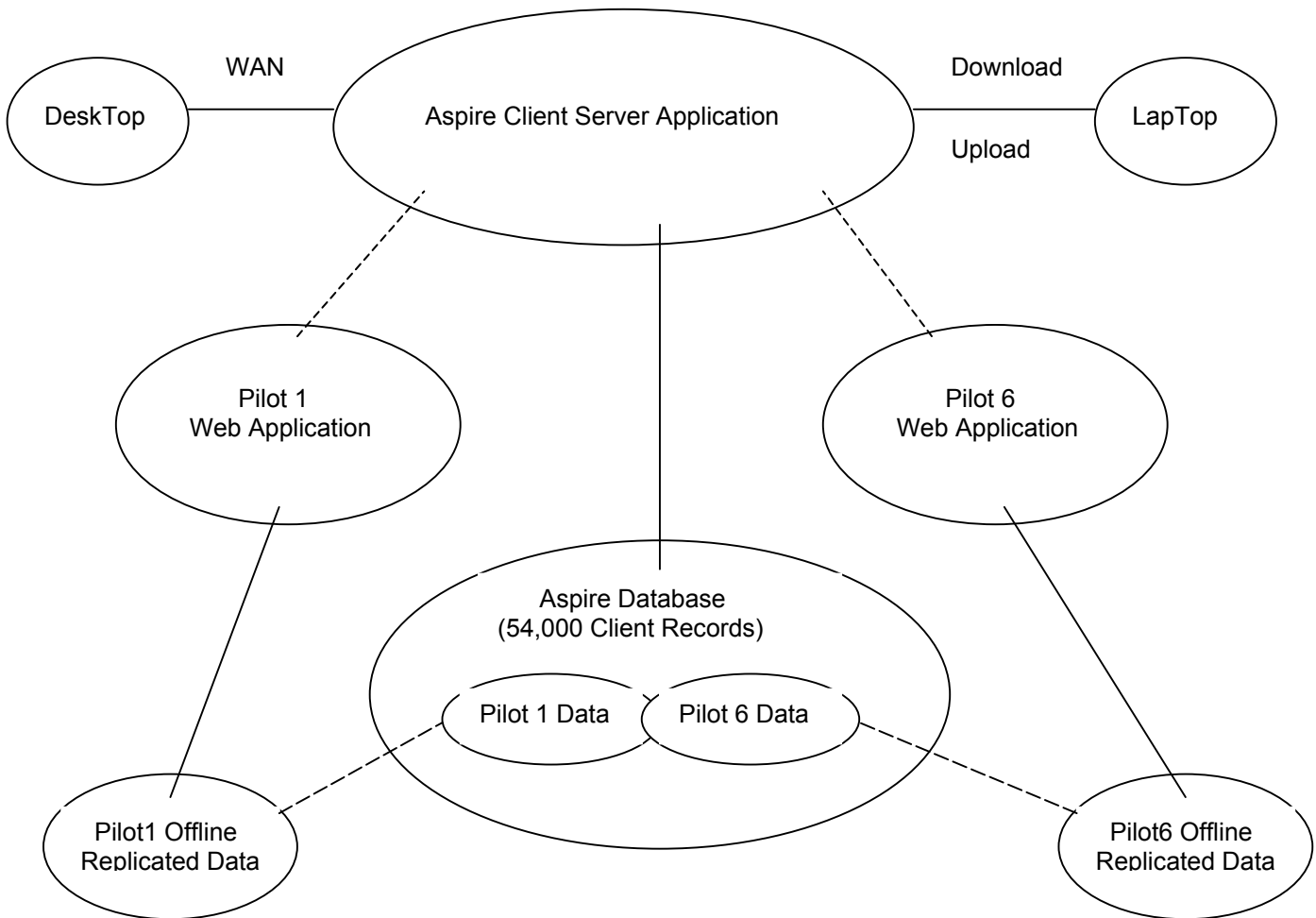
The common cohort of individuals aged between 13 and their 20th birthday, that have the potential to be seen by two or more partners, appears to be in the region of 5,000.

- 2.4 The multi-agency team met several times as a full group over the course of the pilot and between these approval and development meetings, Linda Graham, Bill Cooper, Colin Knowles and Bernie Wiltowski moved the pilot forward. One of the main roles of the multi-agency team was to test shared understanding of requirements but also to disseminate information within partner organisations.
- 2.5 We concentrated on developing the following;
- a data sharing protocol that Connexions organisations could sign up to
 - a client consent form that could be given to young people to obtain their signed consent for sharing sensitive data;
 - options for managing and accessing a shared database of information about young people.

3. FINDINGS

- 3.1 The agencies involved in this project brought with them a depth of understanding in the area of data management and information sharing that had not previously been recognised. Many of the project team had the same personal and organisational concerns and by meeting regularly a trust and understanding has developed across agencies that will form the basis for Connexions in many ways.
- 3.2 We spent a great deal of time deciding on the content of the protocols that will manage the actual process of information sharing but this was valuable both for the reasons above and also because someone needs to do it for all Connexions partnerships. (preferably only once - see section 5)
- 3.3 During the pilot, the national picture did evolve and the potential for a national database is being explored. Our pilot will compliment this work by informing DfEE early in the process about issues that were common to all partners, and particularly clarifying the legal framework within which partnerships have to operate.
- 3.4 We found that the issue of consent largely goes away when young people are asked how they feel about it. A survey on the views of young people conducted by Pilot 2 (Involving Young People and Parents), included questions from us about data sharing. This revealed that young people are happy for data on them to be shared amongst Connexions partners, but would not want this data to be released to their parents.
- 3.5 Developments in service delivery may be slow, as different cultures will need to find their balance. However, the agreements we have been able to reach on protocols, consent and using a common database will help once all agency staff can be trained in common approaches to data and clients information. This will give all practitioners the confidence that they are working legally as well as professionally in the interests of young people.
- 3.6 Proposed Data users can be split into two distinct groups: Connexions Personal Adviser's (PA's) and front-line staff; and staff at partner organisations.
- 3.7 Connexions PA's and front-line staff will need to have full access to Aspire to enable all interactions with clients to be recorded. This is required, if for no other reason, to generate the monthly statistics for DfEE in a timely and efficient manner. Staff at partner organisations will, as a minimum, need to be able to see which clients have had interactions with which organisations and preferably when. This will give them a snapshot view of each client and be used to signpost organisations to one another.

Table 2
Summary of Findings and Proposed Application and Database Structure



PROPOSED APPLICATION AND DATABASE STRUCTURE

The above structure has been designed to enable ALL prospective data users to gain access to the information they require in the easiest way possible and also keep the time to deploy such a solution to a bare minimum. A further advantage is that security is high but with a relatively low maintenance overhead. (Pilot 6 – see 2.1)

To fully understand the structure it must be appreciated that an Application and Database are two separate entities. An application is a tool for viewing and entering data in a timely and efficient manner, and requiring only a limited knowledge of computing. It is not unusual for two or more applications to be attached to a single database, as different end users may well have different data processing requirements but from the same set of data.

3.8 We have had an indication from DfEE that the protocol for data sharing and the client consent form developed from the pilot is capable of use by other Connexions partnerships.

4. KEY LESSONS

- 4.1 This project highlighted the differences between the cultures of organisations that will be working together within Connexions partnerships. We realised that if practitioners found the formal process of data sharing too cumbersome they would actually avoid it. This might not disadvantage the individual young people, where informal data sharing practices are already used, but would hamper service development and in that way ultimately all clients. See 3.7.
- 4.2 For this reason, the technical solution proposed will mean minimum disruption to those whose primary function is not to collect data.
- 4.3 Another major lesson, was to recognise real issues about the legal structure within which personal information can be used. We have consulted widely on this matter and have posed several questions to DfEE that require further investigation for example around parental access to information. We struggled to interpret the Data Protection Act, The Human Rights Act and regulations and guidelines covering organisations such as Social Services and Local Authorities.

5. RECOMMENDATIONS

- 5.1 Clear guidance on the legal framework is sought and this should be published by DfEE. (para. 4.3 above)
- 5.2 Draft protocols and consent forms should be issued for all partnerships to use as a template.
- 5.3 Agencies within Connexions should be given clear messages about their role in Connexions by government departments i.e. there needs to be a cross departmental understanding.
- 5.4 Any development of a national database should be quickly decided upon as partnerships will invest significant money developing their own databases to cope with the demands of tracking.

DATA SHARING PROTOCOL

CONTENTS

PROTOCOL OVERVIEW

TECHNICAL OVERVIEW

DATA SHARING PROTOCOL

CONTEXT

CATEGORIES OF DATA

TARGET GROUP

KEY PURPOSES FOR DATA SHARING

HUMAN RIGHTS ACT

LEARNING AND SKILLS ACT 2000

PRINCIPLES FOR DATA SHARING

DETAILS OF DATA TO BE SHARED

THE SHARED CLIENT DATABASE

CLIENT ASSESSMENT DATA

THE SHARED DATABASE CLIENT GROUP

PROFESSIONAL ETHICS

CLIENT CONSENT

CLIENT CONSENT EXCEPTIONS

CLIENT ACCESS TO RECORDS

RETENTION POLICY

SECURITY

TRAINING

PROTOCOL REVIEW

DECLARATION OF ACCEPTANCE AND PARTICIPATION

PROTOCOL OVERVIEW

This Overview provides a summary of the data sharing arrangements for the Lincolnshire and Rutland CONNEXIONS Service and other Partner Organisations who have signed the declaration of acceptance and participation. All information contained in the overview is subject to the detailed conditions laid out in the Protocol. These conditions include the need for all data sharing arrangements to meet the requirements of the principles set out in the Data Protection Act 1998 and also Article 8 of the Human Rights Act 1998 as described in the Protocol. These conditions also include details of when it may be necessary to share information without the client's agreement e.g. where "the Client is at risk of harm or harming someone else." Parents and guardians have no rights of access to data held on pre sixteen or post sixteen children. All parent or guardian requests to access data must be referred to the designated manager of the relevant organisation/s. These are detailed at the end of the Protocol. Parents and guardians will normally only be able to access data with the signed freely given, specific and informed consent of the client. Access may also be granted in cases where the designated manager is satisfied that the client is not capable of representing themselves and that the parent or guardian constitutes the client's legitimate representative.

The authority for the Connexions Partnerships to collect data on their 13-19 years of age client group is contained in the Learning and Skills Act 2000.

TARGET GROUP:

Those young people in the Connexions Client Group, mainly 13 to 19 year olds, who are not participating in Learning or who are in danger of dropping out of Learning. With respect to the Post 16 Group who opt out of full time further education there are a range of learning opportunities available to them to help them achieve their potential.

CONSENT:

The Client is advised of the legitimate purpose for sharing the data. No data will be transferred without the signed consent of the client or where the client is not capable of representing themselves, the consent of the client's legitimate representative except where the client consent exceptions described in this protocol apply.

Consent will be divided into two parts:

Part One. Signed Client Consent to share the minimum data requirements identified by the Lincolnshire and Rutland CONNEXIONS Service and other Partner Organisations who have signed the declaration of acceptance and participation. Signed Client consent to enter this minimum data on a shared database. To consist of personal data and details of contacts with the above organisations. These are as outlined below and further detailed in the Protocol.

Part Two. Signed Client Consent to share Sensitive data that is additional to that covered by Part One. Unless specifically agreed otherwise with the client, sensitive data would only be shared between professionals directly supporting the client and who have direct contact with the client. This information would be held on the relevant organisations individual databases and not on a shared database.

MINIMUM DATA REQUIREMENTS:

Minimum Data Requirements are to be held on a shared database and/or linked databases (see Technical Aspects Section). These consist of the minimum amount of information identified, which would need to be shared in order to support the client effectively, they further sub-divide into Mandatory and Non-Mandatory Fields (Mandatory underlined). The “Consent Form Held” field indicator is to confirm that a written consent form has been completed and is held on file and will identify which organisation holds the consent form. Minimum Data Requirements to Consist of Client Personal Data and Contact Field Data:

Personal Data (Connexions update only):

<u>Connexions Unique Client Number</u>	<u>Name</u>	Address
<u>Date of Birth</u>	<u>Gender</u>	Address History
Educational Establishment Attended/Attending Code		Employment Status Code

Contact Field Data:

<u>Last Contact Date</u>	<u>Contact Organisation Code</u>	Caseworker/Office Code
Assessment Code	<u>Consent Form Held Indicator</u>	<u>Contact History</u>

TECHNICAL OVERVIEW:

The Shared Client Database to be housed on the Aspire Database with Intranet access for Connexions and other Partner Organisations who have signed the declaration of acceptance and participation. Opportunities for the electronic transfer of some data to be explored where appropriate. A separate Database housing Aggregated Data which organisations subscribing to the protocol wish to share, under terms complying with the requirements of the Data Protection Act 1998, to be accessed using the same links.

DATA SHARING PROTOCOL

CONTEXT

The purpose of the Protocol is to establish a code of practice for the sharing of data which informs and protects partners and clients and adheres to the Data Protection Act 1998 data protection principles and the Human Rights Act 1998. The Protocol itemises the types of data to be shared and used for tracking and referral processes. It is a statement of the principles and assurances, which govern the activity. The term "Partners" refers to those organisations that have signed the Declaration and Participation section of this Protocol. The Declaration and Participation section includes a declaration that the signatory organisation has given notification to the Information Commissioner and that their notification is current.

The authority for the Connexions Partnerships to collect data on their 13-19 years of age client group is contained in sections 114 – 122 of the Learning and Skills Act 2000 (Appendix A).

This protocol is not intended to replace or supersede other protocols written by subscribing partner organisations.

CATEGORIES OF DATA

Data can be summarised into three categories:
See Appendix B for full details of these.

- **Aggregated data** – Statistical representation (e.g. of volumes by geographical area, gender, ethnicity etc)
- **Personal Data** – defined as specific information pertaining to the individual (e.g. age, date of birth, gender, qualifications held, recorded skills and abilities, educational establishment attending/attended, employment history etc)
- **Sensitive Data** – defined as information of both a personal and sensitive nature. For the purposes of this protocol, Sensitive Data consists of two parts. Part one consists of that detailed in the Data Protection Act 1998, that is racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health, sexual life, criminal proceedings or convictions. (See Appendix B for full description). Part two is Professional Sensitive Data. This consists of data not detailed in the Data Protection Act 1998 that is identified as being of a personal and sensitive nature by the individual organisations subscribing to this Protocol. To include history of abuse, care history, school attendance problems, substance misuse, financial status. Sensitive Data detailed in the Data Protection Act 1998 cannot be processed unless a schedule 2 and a schedule 3 condition are met. Signatories to this protocol agree that Professional Sensitive Data will not be processed unless a Data Protection Act 1998 schedule 2 and a schedule 3 condition are met.

In addition:

Aggregated data

Information from which no individual person can be identified is outside the Data Protection Act and may be passed to relevant organisations for bona fide purposes. In all cases this information is to be in aggregate form and those processing such information will need to ensure aggregation is sufficient to ensure that individuals cannot be identified. Individual level information may also be de-personalised (and therefore be outside the ambit of the Data Protection Act) by the removal of all identifying information. Partnerships should note however, that information is still identifiable if it contains unique numbers or other keys that allow it to be separately merged with identifying information (e.g. names) or where identifying information can be looked up.

Statistical Information on volumes of clients by gender, race disability and status can therefore, be shared by the organisations identified in this protocol provided no individual can be identified.

Personal Data

Personal data relates to an individual who is identifiable from that data (or that data in conjunction with other data the data controller holds or is likely to obtain): a reference number is personal data if it can be linked with an individual's name elsewhere in an organisation. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. All types of personal data are within the ambit of the Data Protection Act. Personal Data is to be processed in accordance with the 1st Data Protection Principle (see Appendix B). Clients must be advised of the reason for this collection, rationale for any sharing of the data and the other organisations with which it may be shared.

Sensitive Data

Partnerships will need to have particular regard for whether the personal information they are processing is sensitive personal information, for which more stringent controls are needed as detailed above (and in Appendix B). Partnerships will wish to be aware that in some cases simply the name and address of a young person will be sensitive. For example, if it arises from a source that in itself identifies a young person as having a characteristic that is included within the definition of sensitive personal information.

For the purposes of this protocol with regard to the shared database and joint case-working the following applies. Sensitive data will only be collected and shared with the express permission of clients who must be advised of the reason for its collection, rationale for any sharing of the data and the other organisations with which it may be shared. The exceptions to this are detailed under the “Client Consent Exceptions” section of the Protocol. This “Client Consent Exceptions” section also details the procedures that must be adhered to in such cases.

TARGET GROUP

Those young people in the Connexions Client Group, mainly 13 to 19 year olds, who are not participating in Learning or who are in danger of dropping out of Learning.

Those in the target group often share multiple problems and are likely to be members of one or more of the following groups:

- care leavers (certain groups)
- young offenders
- truants
- travellers
- excluded clients
- clients with special needs
- clients underachieving
- substance misusers
- teenagers pregnant
- clients at risk of significant harm
- teenage parents
- young carers
- children in care (certain groups)

KEY PURPOSES FOR DATA SHARING

- For Partners who have signed the declaration of acceptance and participation to share data on clients for the benefit of these clients.
- For Partners who have signed the declaration of acceptance and participation to share aggregated data for agreed reasons. Typically to include information required for statistical government returns, including management information required by the Connexions Service National Unit, and information identified as needed for local and regional planning purposes e.g. for Learning and Skills Council planning purposes.

HUMAN RIGHTS ACT 1998

The following notes provide additional guidance and requirements for partner organisations subscribing to this Protocol but do not override their obligations to adhere to the principles and procedures listed elsewhere in this protocol.

The following is an extract from The Human Rights Act 1998: Guidance for Connexions Partnerships (DFEE)

APPENDIX 1

The Human Rights Act 1998 makes it unlawful for a public authority to act in a way that infringes an individual's rights and freedoms under the Act. "Public Authority" is given a wide meaning and it is likely that a court would hold that Connexions Partnerships are public authorities for the purposes of the Human Rights Act even though one might not regard them as in the "public sector" in the traditional sense.

When a Connexions Partnership is in any doubt about their obligations under the Human Rights Act they should take their own legal advice

The Human Rights Act 1998 aims to "bring home" the protection of rights set out in the European Convention. It does this by:

- requiring public authorities to act in a way that is compatible with Convention Rights;
- requiring the courts to interpret statute and common law in accordance with Convention rights wherever possible;
- requiring that sponsors of new legislation make declarations when introducing the Bill in Parliament as to the compatibility of that legislation with Convention rights.

In general, as long as Connexions Partnerships work within the guidelines the DFEE has set out the likelihood is, in the Department's view, that they will comply with the Human Rights Act. When a Connexions Partnership is in any doubt about their obligations under the Human Rights Act they should take their own legal advice.

There are two areas where queries have been raised about Connexions Service activity that may be relevant to the Act – the sharing of information (Article 8) and focussing on certain groups of young people (Article 14).

- 1 Sharing of information.** Article 8, gives the right to respect for private and family life, home and correspondence. However this can be breached where legislation allows and it is necessary for **HRA six conditions**. This should not hamper personal advisers from sharing information in order to carry out their duties. This includes professionals holding verbal discussions about individual young people, as long as they give due respect and consideration to privacy and confidentiality. However, it is considered good practice to inform the young people that these discussions are taking place. Of more relevance is the guidance that is already in place covering record keeping and the disclosure of information. The principal other legislation covering this field is the Data Protection Act and Services who comply with those requirements will be complying with the principles of Article 8.
- 2 Targeting provision and support.** Article 14 prohibits discrimination in the enjoyment of the Convention rights. Targeting resources to those young people who are the most vulnerable should not be in contravention of the Act because before Article 14 can apply the enjoyment of some other Convention right must be at issue. There is an obligation for Connexions to provide a universal service. Services must respond to all requests by young people in their client group and provide them with the information, guidance and support that is appropriate to their needs. The essence of the targeting service is that for certain vulnerable groups, the service must be proactive in seeking them out and offering them help to ensure their rights under Article (**see Colin**)

LEARNING AND SKILLS ACT 2000

Section 114 (4) of the Act states that "Young Persons" means persons who have attained the age of 13 but not the age of 20.

Sections 114 - 122 of the Learning and Skills Act 2000 provide the framework which allows the establishment of the Connexions Service. In particular, Section 117 sets out the duties on maintained schools and LSC funded providers to provide relevant information, Section 119 enables disclosure of some social security information, and Section 120 Subsection (2) lists persons and bodies empowered to supply relevant information about young people:

Local Authority; Health Authority; Learning and Skills Council; Chief Officer of Police; Probation committee; Youth Offending Team; Primary Care Trust.

Section 120 facilitates the lawful sharing of information by the bodies there mentioned in pursuance of the services specified in section 114(1) of the Act; "that is services which (the Secretary of State) thinks will encourage, enable or assist (directly or indirectly) effective participation by young persons in education or training."

PRINCIPLES FOR DATA SHARING

- client permission will be sought prior to any transfer of sensitive data
- access to client data will be restricted to the "need to know" principle
- only the minimum information required for the purpose stated will be transferred
- the purpose for use of personal/sensitive information will be justified
- staff accessing personal/sensitive data will be trained and accept their responsibilities in relation to handling client data
- clients will be able to see on their personal records details of information transferred and why
- data will only be used when necessary
- the systems for transferring data and the need for data transfer will be subject to ongoing review
- data transferred will be accurate and non subjective (unless qualified)
- where any inaccuracy is brought to notice the error will be corrected and the originating partner will be responsible for circulating the corrected information to all agencies to whom the inaccurate information had been sent

DETAILS OF DATA TO BE SHARED

It is not in the client's interest and not permissible for sensitive information to be transferred unless the principles stated in the "Principles for Data Sharing" section above apply. Therefore the intention of the organisations that subscribe to this protocol is to provide initial data to each other which identifies clients that each is working with who are categorised as being "at risk of dropping out of learning" or "who have dropped out of learning." With respect to the Post 16 Group who opt out of full time further education there are a range of learning opportunities available to them to help them achieve their potential.

The purpose behind this activity is to help each organisation identify whether clients are already known to them and whether activity is already underway or intended to take place with those clients to help them engage or re-engage in learning.

The data to be shared divides into the following:

Aggregated Data to assist strategic planning and reporting

Aggregated data can be shared as detailed in the Data Protection Act section of the protocol. In addition partner organisations subscribing to the Protocol will adhere to the following:

- Aggregated data will not be used or merged to identify individuals
- Data will not be passed on for commercial activities or purposes without the originators specific written consent
- If data is to be used by any third party, specific written consent must be gained from the originator

Where a partner organisation subscribing to the protocol wishes to access or generate Aggregated data, not currently available, an Aggregated Data Request Form may be completed detailing:

- Aggregated data required from partner organisations (to include type of data, target group, format required, date needed by etc)
- Authority/Purpose/s for acquiring each set of data
- Aggregated data to be produced
- How data will be used
- Data recipients – Details of organisations or individuals who will have access to or receive information
- How data can be accessed and shared by partner organisations subscribing to this protocol, including details of any proposed embargo or proposed specific restrictions on use

Personal Client Data

The personal client data to be held on the shared client database detailed in the following section forms the agreed minimum amount of data identified by the organisations subscribing to this protocol which would need to be shared in order to effectively support clients in the target group. The “Consent Form Held” field indicator is to confirm that a written consent form has been completed and is held on file and will identify which organisation holds the consent form.

Equal Opportunities Monitoring Data

Data on ethnicity and special needs is categorised as sensitive data and is not held on the shared database.

Aggregated data resulting from equal opportunities monitoring from which no individual person can be identified will be shared by Connexions with partner organisations.

Connexions will use this data for the following:

- To monitor any patterns of disadvantage or discrimination that correlate to membership of a particular group.
- To ensure that all clients are enabled to access the information, guidance advice and support that they are entitled to, from Connexions in order to meet their individual needs

Sensitive Client Data

The following data fields held on the shared database can be classified as sensitive data either under the Data Protection Act 1998 or under Professional Sensitive Data (as outlined in the “Categories of Data” Section of this Protocol):

Contact organisation details, caseworker details, assessment details, employment status and an address or education establishment which identifies a young person as having a characteristic that is included within the definition of sensitive personal information. These fields constitute the limit to the range of sensitive personal data to be held on the shared database.

Indicator and contact codes to be used to maximise data security and confidentiality. Sensitive Client Data, which goes beyond the limits of that listed above, will not be held on a shared database.

Sensitive data can only be collected and shared, in accordance with the legal requirements detailed in the “Data Protection Act” section and other sections of this protocol.

Unless specifically agreed otherwise with the client, sensitive data that goes beyond that held on the shared database, would only be shared between those professionals directly supporting the client and who have direct contact with the client. Professionals recording this sensitive data would do so on their own organisations individual database.

Data Sharing Arrangements

The mechanisms and processes for transferring data from partner organisations to a Connexions shared database are detailed in Appendix C along with arrangements for updating data on the shared database. These to be agreed individually with each organisation and signed by the designated manager for that partner organisation.

THE SHARED CLIENT DATABASE

The Shared Client Database is used to store the Minimum Data Requirements. These consist of the minimum amount of information, which would need to be shared in order to support the client effectively.

Mandatory and Non-Mandatory Fields

It is accepted that the level of sensitivity of the data held in a number of the data fields may vary both in terms of the data itself and in terms of the organisation inputting the data. In recognition of this the data fields are further split into Mandatory and Non-Mandatory categories.

Mandatory:

Connexions Unique Client Number, Name, Date of Birth, Gender, Last Contact Date, Contact Organisation Code, Contact History, Consent Form Held Indicator.

Non-Mandatory:

Address, Address History, Educational Establishment Attended/Attending, Employment Status Code, Caseworker/Office Code, Assessment Code.

The Minimum Data Requirements also forms the limit of client data to be held on a shared database.

The data held comes under the following broad headings:

Personal Data (Connexions update only):

Connexions Unique Client Number	Name	Address
Date of Birth	Gender	Address History
Educational Establishment Attended/Attending Code		Employment Status Code

Contact Field Data:

Last Contact Date	Contact Organisation Code	Caseworker/Office Code
Assessment Code	Consent Form Held Indicator	Contact History

The database will be updated in line with the Connexions data review and disposal policy agreed with individual partners subscribing to this protocol.

CLIENT ASSESSMENT DATA

Client Assessment Data can be classified as sensitive data. The Assessment Code field is a non-mandatory field on the Shared Client Database.

With regard to the Shared Client Database organisations subscribing to this protocol will be able to enter Codes into the Assessment Code Field to show the following:

- An individual client has undergone an assessment (general code).
- An individual client has undergone an assessment process using a specific diagnostic tool or process, which is identifiable by its code (specific code).
- An individual has undergone an assessment and has completed a consent form giving their permission for the originating organisation to share a professional interpretation of the results with specified other organisations, providing they are both subscribing to this protocol and working directly with the client (general or specific code plus consent code).

Each individual organisation subscribing to this protocol will need to identify whether or not they wish to complete the Assessment Code field and if so whether they would use only the general code or specific codes or a general or specific code plus the consent code.

Codes identifying specific assessment/diagnostic tools will need to be agreed with the relevant organisations.

THE SHARED DATABASE CLIENT GROUP

The shared database will only consist of those advised and consenting clients of organisations that have subscribed to a data sharing protocol with Connexions. The shared Connexions database will consist of those young people in the Connexions Client Group with whom one or more Partner organisations are working with, and who fall into one of the target group “at risk” categories.”

PROFESSIONAL ETHICS

All staff will be sensitive to the need for inter-agency confidentiality when discussing clients with the other partners identified in this protocol. In order to help the clients, it may be necessary for professionals to discuss client details. Information passed verbally still constitutes a disclosure and a processing of information. Its use must be agreed at the time by the individual professionals involved in particular how/if it will be recorded and acted upon. The Client Consent Form details the need for professionals to pass on information to a range of organisations in order to benefit the client. The client (or their legitimate representative) will need to have signed the client Consent Form before the disclosure described in this section can take place.

CLIENT CONSENT

It is essential that the collection of data held on clients by each organisation as well as the transfer of data to the other organisations subscribing to this protocol complies with the provisions of the Data Protection Act and the Human Rights Act. Organisations subscribing to this protocol must also have given notification to the Information Commissioner and their notification must be current.

In gaining client consent to share data the client must be advised of the reason and rationale for any sharing of the data and the other organisations with which it may be shared.

Client consent is divided into two parts. Both parts require the client to sign the relevant Client Consent Form. Both parts state the Client has the right to give notice of their withdrawal of consent at any time.

Part One. Signed Client Consent is needed to enter the client's details onto the shared database where the minimum data requirements as outlined above may be recorded. **This client consent form includes details of the reasons and purposes for collecting the sensitive data on ethnic origin and special needs.** This information would be accessible to all the organisations subscribing to the protocol. A copy of the client consent form would be kept by the originating organisation and the "Consent Form Completed indicator" entered on the shared database. A copy of the client consent form would be forwarded to the shared database controller.

Part Two. Signed Client Consent is needed for organisations to collect and share any sensitive data on the individual client that is additional to that covered by Part One. This to include Sensitive data as detailed in the Data Protection Act 1998 and Professional Sensitive Data as defined in the "Categories Of Data" section. This details the individual organisations that may share sensitive data on the client. Only the individual organisations detailed would share sensitive data. Each organisation will also ensure that any subsequent transfer of sensitive data receives, or has the clients signed consent.

A new Client consent form would need to be signed if a further organisation wished to collect or share sensitive data on the client.

In relation to sensitive data a copy of the Client Consent form will be kept by each organisation for the duration that they keep the Client record.

Sensitive data can only be collected and shared with the express permission of clients who must be advised of the reason for its collection, rationale for any sharing of the data and the other organisations with which it may be shared, in accordance with the legal requirements detailed in the "Data Protection Act" section of this protocol.

Professional judgement must be used to ensure that only relevant data is processed. Data would normally be defined as relevant where it's recording and processing can be used to better support and benefit the client, and/or for clear reasons of health and safety in relation to the client and those working with the client (see also "client consent exceptions" section below). All cases where the relevance of collecting or sharing data is in doubt must be referred to a designated manager within the organisation.

Where a client cannot sign a consent form a signed statement that the client has given consent must be provided by the member of staff requesting consent and countersigned by a designated manager within that organisation.

In cases where the designated manager is satisfied that the client is not capable of representing themselves and that the parent or guardian constitutes the client's legitimate representative the signed consent of the parent or guardian should be obtained.

CLIENT CONSENT EXCEPTIONS

Sometimes it will be necessary to share information without the client's agreement. Detailed below are the cases where this may be necessary:

- The disclosure prevents the client committing a criminal offence that could place others at risk or places the Personal Adviser/other Professional at risk of collusion
- The client is at risk of harm or harming someone else
- The client needs urgent medical treatment
- The client is behaving in an abusive, discriminatory or violent way
- Connexions is ordered to give information as part of a legal proceeding

NB Requests from the Police Force for data to enable them to pursue an investigation will only be provided on receipt of a Section 29 (3) Form.

Each organisation will implement procedures for and identify a designated manager or managers with the authority to make decisions with regard to circumstances requiring disclosure without client consent as outlined in the above circumstances.

All situations where it may be necessary to breach client confidentiality must be referred to a designated manager unless exceptional circumstances apply e.g. where urgent treatment is required or there is immediate risk of harm. The reason/s for breaching client confidentiality must be fully recorded and clearly referenced to the evidence and information on which the decision is based. This must be recorded, including details of any third parties and the information/evidence they have given.

CLIENT ACCESS TO RECORDS

Clients may request the details of their records at any time by putting their request in writing. Parents and guardians have no rights of access to data held on pre sixteen or post sixteen children. All parent or guardian requests to access data must be referred to the designated manager of the relevant organisation/s. These are detailed at the end of the Protocol. Parents and guardians will normally only be able to access data with the signed freely given, specific and informed consent of the client. Access may also be granted in cases where the designated manager is satisfied that the client is not capable of representing themselves and that the parent or guardian constitutes the client's legitimate representative.

Under the Data Protection Act:

On making a request in writing (including electronic means) to the data controller, data subjects have the right:

- To know that their personal data is being processed by the data controller, to be given a description of that data, the purpose(s) for which it is being processed and to whom the data is or may be disclosed.
- To be supplied with a permanent copy of the data in question, and an explanation of the data if it is not intelligible to them. They also have the right to be given information about the source of the data, though the data controller might not be obliged to make this available if this would identify another individual. For further information see section 7 of the Data Protection Act 1998.
- Personal data relating to an individual must be provided within forty days of the receipt of a written request and on receipt of the appropriate fee. The maximum fee chargeable has been set by regulations at £10.

RETENTION POLICY

The right to hold data on clients that has been transferred without permission could be challenged. Consent forms must, therefore, be retained by the organisations identified in this protocol as proof of permission. Consent forms should be retained by organisations for the duration that they keep client records.

With regard to consent forms for the shared database the centrally held form will be retained while data is held on the client by Connexions. Data will be held on clients up to the client's 20th Birthday. Where a client has identified special needs Connexions will continue to support the client up to the clients 25th birthday or until the client has been in a settled destination for a 3 to 6 month period. Data will only be kept beyond age 20 for those clients with special needs with their consent or that of their legitimate representative.

SECURITY

Each organisation will designate an appropriate manager or managers to act as the named recipients of transferred data as outlined below.

All data transferred under the data sharing arrangements drawn up in this protocol must be transferred in accordance with the procedures agreed with each partner organisation as detailed in Appendix C.

This transferred data may be stored electronically subject to normal database security procedures.

Each recipient will ensure that the data is stored securely within their organisation and made inaccessible to the public/non-relevant staff both when in and not in use.

TRAINING

All the partners subscribing to this protocol will:

- Share this protocol within their individual organisations with all staff involved in direct or indirect receipt of transferred data
- Train staff to meet the requirements of the protocol
- Document procedures to implement the Protocol.

PROTOCOL REVIEW

This Protocol to be reviewed on an annual basis. The review to be carried out by a Senior Manager from each of the organisations subscribing to this protocol. To include a review of the shared database and the Connexions data review and disposal policy agreed with partners subscribing to this protocol.

DECLARATION OF ACCEPTANCE AND PARTICIPATION

We the undersigned, on behalf of our stated organisation, agree to support the implementation of this Data Sharing Protocol through the provision and management of data in accordance with the conditions detailed in this protocol. We declare that we have given notification to the Information Commissioner and that this notification is up to date and reflects our current use and storage of data.

Signed..... Date.....

Name.....

Organisation.....

Address.....

.....

.....

Signed..... Date.....

Name.....

Organisation.....

Address.....

.....

.....

TECHNICAL SUB GROUP REPORT

CONTENTS

Overview and Format of Report

Role No1 Findings

Role No1 Recommendations and Considerations

Role No2 Findings, Recommendations and Considerations

Role No3 Findings, Recommendations and Considerations

Summary and Proposals

Overview

Role of Group

1. To identify the possibilities in relation to getting in place a secure shared client database that can be accessed by a range of agencies that will have signed the data sharing protocol.

The shared client database to ideally be the Aspire database. Access to data to be restricted to certain information fields for some clients only.
Access to be based on an Extranet system.

2. To identify the possibility of secure internet/intranet access to shared Aggregated information site or sites (exploring using the Lincolnshire Research Observatory).
3. To investigate the scope for linked access to the Shared Client Database, Aggregated Information Database, Diagnostic Tools and Assessment Database (being developed for Pilot 6 by Tony Roberts).

Format of Report

This report has been written after attending various meetings at which partner organisations have been represented and also contacting members of Pilot 1 Technical Sub-Group.

Each of the above Roles will first be dealt with separately, outlining Findings, Recommendations and Issues for consideration. Then, any linkages between the Roles will be identified within the report summary.

Role No1

To identify the possibilities in relation to getting in place a secure shared client database that can be accessed by a range of agencies that will have signed the data sharing protocol. The shared client database to ideally be the Aspire database. Access to data to be restricted to certain information fields for some clients only.
Access to be based on an intranet system.

Findings

Users and their Requirements

Proposed Data users can be split into two distinct groups:

- Connexions Personal Adviser's (PA's) and Front-Line staff.
- Staff at Partner Organisations.

Connexions PA's and front-line staff will need to have full access to Aspire to enable all interactions with clients to be recorded. This is required, if for no other reason, to generate the monthly statistics for DfEE in a timely and efficient manner.

APPENDIX 2

Staff at partner organisations, will as a minimum, need to be able to see which clients have had interactions with which organisations and preferably when. This will give them a snapshot view of each client and be used to signpost organisations to one another. This methodology seemed to be most acceptable, in principle, to most partners.

It should also be noted that a number of PA's are likely to be recruited from partners and could well be working for Connexions on a secondment basis.

Finally, it is envisaged that there will eventually be between 80 and 100 PA's who will be based all round the two counties, with some of them located in schools. A definitive list of numbers and locations though, is not currently available.

Aspire

Aspire is the database application currently used by LC&GS and will continue to be used by Lincolnshire and Rutland Connexions Service. It is windows based and uses Microsoft SQL7 to store the data, with tools available to easily access this data for reporting purposes.

Aspire can be run over a Wide Area Network (WAN), with 9 county based offices currently connected to the SQL Database Server at Witham House in Lincoln.

There is also the facility to download restricted data sets to a lap top computer and then upload this data back to the main file server. However, no new records can be added and only specific amendments can be made. This process is also very time consuming at present. This should be resolved with the issue of SQL service pack 3 and Aspire version 01.04, making this function a more realistic option if stringent controls are put in place.

At present, different users can be assigned varying access rights, but these restrictions cannot be taken down to "Client" or "Field" level.

Finally, it should be noted that this product is not "Web Enabled" and cannot therefore be run over an Intra/Extra Net.

Data Currently Available in Electronic Format

Below is a table highlighting what data is collected and by which partner organisations, plus other important information.

Data Held	Organisation								
	LCC	RCC	EWS	SSD	YOT	POL	YS	LCGS	LTEC
Name	Some	Yes	Yes	Yes	Yes	Yes	Some	Yes	Yes
Address	Some	Yes	Yes	Yes	Yes	Yes	Some	Yes	Yes
DoB.	Some	Yes?	Yes	Yes	Yes	Yes	Some	Yes	Yes
Gender	Some			Yes				Yes	Yes
Ethnicity	Some			Yes	Yes		Some	Yes	Yes
Disability	Some			Yes			Some	Yes	Yes
School	Some	Yes	Yes	Some	Yes		Some	Yes	
College					Yes		Some	Yes	Yes
Workplace					Yes		Some	Yes	
Age	3 - 19	4 - 16	5 - 16	0 - 100	10 - 17	0 - 100	11 - 25	13 - 25	16 - 25
Cohort Size	100,000	4,500	5,000	70,000	532	Unknown	Unknown	54,000	4,500
Cohort Size 13-20				4,000	532	Unknown	Unknown	54,000	3,500
Dbase Client ID	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes
CSV Export	Yes	Yes??	No???	Yes	Yes???	No	No	Yes	Yes
Internet Access	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes

Lincolnshire County Council (LCC) is at the moment developing a new student database that is not planned to be fully functional until February 2002. This means that in the short-term there is no single definitive listing of school pupil data other than that held by LC&GS.

The Youth Service (YS) tend to collect data in paper format, although some stand-alone databases do exist.

The common cohort of individuals aged between 13 and their 20th birthday, that have the potential to be seen by two or more partners, appears to be in the region of 5,000.

Recommendations and Issues for Consideration

User Access and Aspire

As already highlighted in the findings, the potential users of Client Data can be easily split into two distinct groups. It therefore makes sense to explore the possibilities of providing two solutions to the data-sharing problem. The solutions that I propose are as follows:

Recommendation

Connexions PA's and Front-Line staff should all be given full access to Aspire through a WAN link. However, at present there are only WAN links to the 9 offices around the county. This means that at a bare minimum we need to set up a WAN link to Oakham in Rutland and also to a large number of secondary schools, if that is where PA's are to be based.

Considerations

To help reduce costs and make best use of existing infrastructures, Jorg Walther LC&GS IT Officer, has contacted Geoff Chandler to investigate the feasibility of connecting our WAN to the one being developed for the National Grid for Learning (NGfL) within Lincolnshire. The outcome of this meeting was positive with an agreement in principle being reached. It should be noted though, that WAN connections to the vast majority of secondary schools within Lincolnshire will not be completed until end of July 2001. This should not cause any major problems though, as I understand that the roll-out of PA's to be based at schools is over a longer time frame.

If PA's in Rutland are to be based in schools then we would need to have WAN links installed ourselves. Although there are only 3 secondary schools and a sixth form college in Rutland.

There could also easily be 'Loading' issues with our current WAN infrastructure and upgrades may be required to the WAN links themselves, cabling in satellite offices and/or the SQL Database Server at Witham House. One area of major concern is the WAN link between Witham House and Hyder which is only a 389k line. This equates to approx 40 users if Ideas Integrations' figure of 10k per user is accurate.

Greater use of the laptop upload/download routine could be considered if V01.04 of Aspire cures the timeout problems. However, strict protocols would need to be adhered to, to ensure data integrity.

It should be noted that until numbers of users and their locations is available, it is not possible to ensure that the correct infrastructure is in place.

It has been suggested that a fully web enabled version of Aspire would resolve these communications problems. Although this might be true, the lead-time and costs to develop such a system would be prohibitive.

Recommendation

To give **Staff at Partner Organisations** a signposting system to see interactions between organisations I would propose that we commission Ideas Integration to develop their Aspire on the net Client Search application.

The available data would be kept to a bare minimum containing Name, Date of Birth, Address and Gender, on one screen, and a flagging system to denote organisations contacted on a second. The number of flags to be set for each partner organisation will range from 500 to 5,000 which means that setting these manually would be a very time consuming affair. I would therefore suggest that this should be automated, with each partner providing data in a specified format. Updates would need to be carried out on at least a monthly basis.

Considerations

Such a development would take approximately 3 months to write, test and deploy. Costs as yet are unknown.

I would suggest that for security reasons this application did not access the Live Aspire database but instead looked at a separate database that contained only the base information described above. This is not technically too difficult and could be easily updated on a daily basis. It would also make sense to have this application and database installed on a dedicated web server in Witham House, again for security reasons and also for ease of maintenance.

This application could well have a declining user base if PA's are seconded from partner organisations. Usage could also diminish as we start to more fully map interactions with clients from age 13.

Users of the system would need access to a web browser, which might be problematic in the short term even for partners working from their dedicated office.

The system will only be as good as the data available. If partners want to be able to see fields such as "Consent Form Held", then protocols will need to be adopted to ensure timely and accurate updating, whether on a live basis or through update routines. This could lead to some dual processing as partners could already be entering this data onto their own systems.

If data from Aspire is to be used to populate this system then partners should be aware that if sensitive data is made available then it might not exactly match the data they hold on certain clients. Do we want to put a procedure in place to cover such eventualities?

Considerations for both Options

Current staffing levels would need to be reviewed, as we do not necessarily have sufficient staff with all the knowledge required to deploy these systems.

There will be a significant training requirement for both Connexions and partner system users.

Further development of Aspire will be required if the data sharing protocol is to be fully implemented. e.g. Address History.

Pilot 6 requirements should not be forgotten if we are to develop a fully integrated solution. (See Role No3 for requirements)

Role No2

To identify the possibility of secure internet/intranet access to shared Aggregated information site or sites (exploring using the Lincolnshire Research Observatory).

Findings

The Lincolnshire Research Observatory (LRO) is a web based information system being developed by a partnership between Lincolnshire Development (part of LCC) Lincolnshire Health Authority and Lincolnshire Police, with a further 19 organisations currently showing an interest in the project.

Its aim is to act as a single point for data and information on the County, improve the availability and use of that data and information, raise levels of expertise and capacity amongst the partner organisations, reduce duplication of effort for data 'providers' and research fatigue amongst client groups. It will also provide links to existing websites and networks across the County and Region, providing a seamless approach to the provision of data and information to the end user.

Data security is obviously of great importance and much work has been done in this area, with Lincolnshire Police having invested approx £17,000 on a server to protect their data from being hacked into. Within the web site there are restricted areas that can only be entered if you have the appropriate access rights. In addition to the site security it is also possible for partners to have links back to their own sites to enable them to use their own security through firewalls or passwords.

The one main advantage of the LRO is that data can be published using the GIS (Geographical Information System) software that they have. This means that any data supplied containing Lincolnshire postcodes can be displayed on a map of Lincolnshire. At present Rutland is not available but could be added, at additional expense, if required.

Recommendations and Issues for Consideration

The LRO seems to be an ideal tool to enable Lincolnshire and Rutland Connexions Service to publish statistics for both internal and external consumption. The GIS software is particularly exciting and would enable publication of outcomes or uptake by geographic areas down to ward level. The only limiting factor could well be one of resourcing.

Role No3

To investigate the scope for linked access to the Shared Client Database, Aggregated Information Database, Diagnostic Tools and Assessment Database (being developed for Pilot 6 by Tony Roberts).

Findings

The requirements of Pilot 6 draw heavily on the outcome of Pilot 1, both with regards to the data sharing protocol and the technical solution to giving Connexions staff and partners access to the relevant levels of data.

To date a Microsoft Access database has been written with users gaining access to this through a Web enabled front-end. The database contains a wealth of Diagnostic Instruments that are categorised into one of three groups, depending on the level of practitioner qualifications to enable their use. These groups are then used to set the security rights of each user.

On initial contact with a client, a practitioner will need to check:

- previous assessment contact and history
- previous action plans held within Aspire
- if there have been any interactions with partner organisations

Each time a Diagnostic Instrument is used with a client, this interaction and its outcome(s) needs to be logged. This could also involve the completion of a new action plan, which would need to be logged on Aspire.

To enable Pilot 6 to function effectively there is a need for users to have access to view and update data that is currently held on the Aspire database.

Recommendations and Issues for Consideration

Recommendations

To help reduce the need for users to have to log into Aspire to check or update data it would be useful if the Pilot 6 software was written to enable a data Download / Upload routine to be run. This could work in a similar way to the present laptop routine.

It makes sense to continue development of a web-enabled solution as this links well with the recommendations for Pilot 1.

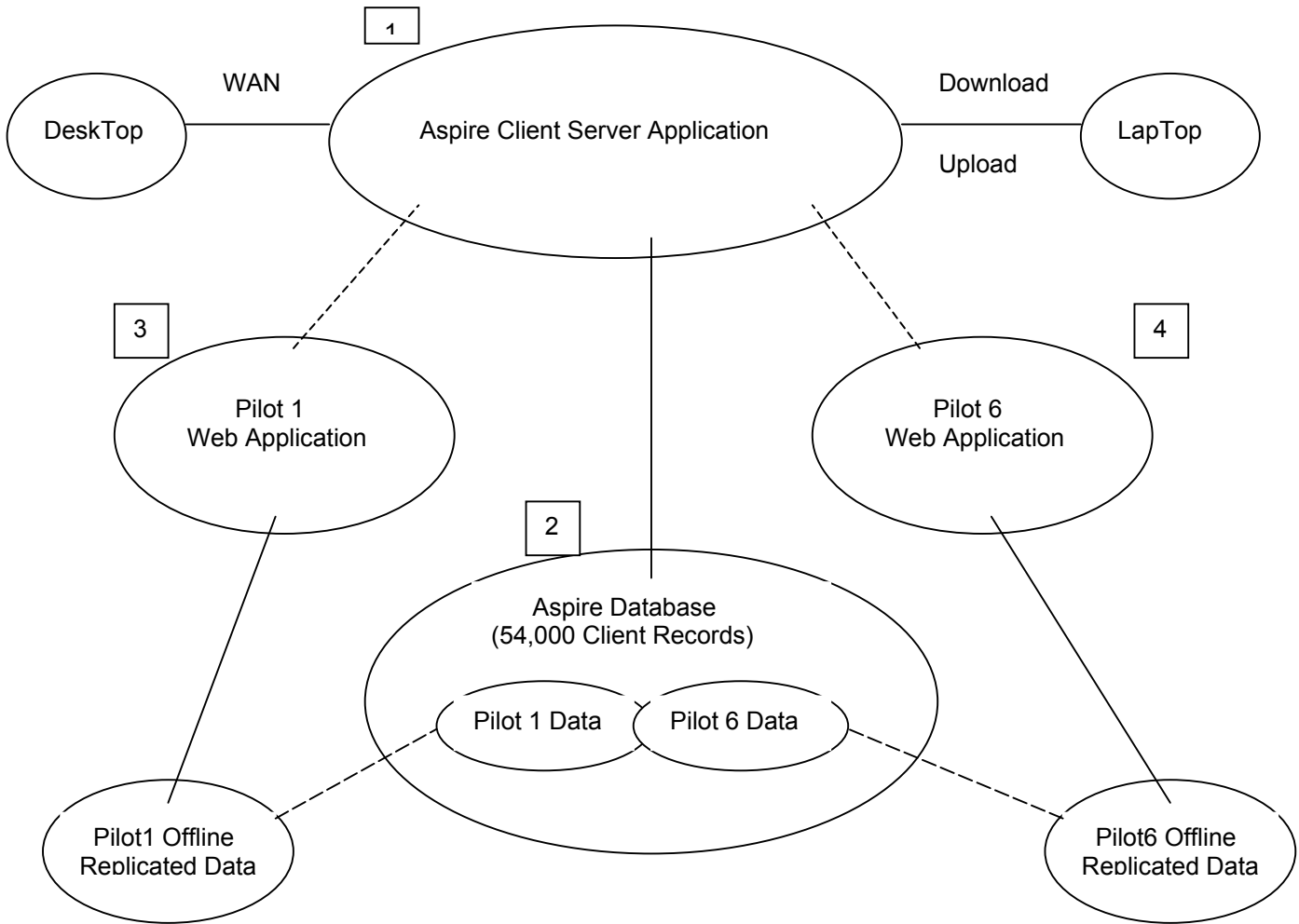
It is imperative that Pilot 1 and Pilot 6 continue to move forward together.

Considerations

If a Download / Upload routine between Aspire and Pilot 6 is to be developed, then there will need to be collaboration with Ideas Integration.

Additional fields will need to be created within the Aspire database if an integrated approach is adopted.

Summary of Findings and Proposed Application and Database Structure



PROPOSED APPLICATION AND DATABASE STRUCTURE

The above structure has been designed to enable ALL prospective data users to gain access to the information they require in the easiest way possible and also keep the time to deploy such a solution to a bare minimum. A further advantage is that security is high but with a relatively low maintenance overhead.

To fully understand the structure it must be appreciated that an Application and Database are two separate entities. An application is a tool for viewing and entering data in a timely and efficient manner, and requiring only a limited knowledge of computing. It is not unusual for two or more applications to be attached to a single database, as different end users may well have different data processing requirements but from the same set of data.

1 Aspire Client Server Application

All front line delivery staff will have access to Aspire regardless of their place of work. Anyone based at a satellite office will be able to use a desktop pc, viewing and amending records in real time over our existing WAN.

For those members of staff that require access to data while out of the office, a laptop will need to be made available. This will allow them to use the Aspire download routine to take the records of the individuals that they are likely to be seeing with them. After making any amendments, and on return to a satellite office, the data will then need to be uploaded back into the Aspire database.

2 Aspire Database

The database will contain a record of all 13 to 19 year olds who are resident in Lincolnshire or Rutland, plus those aged between 20 and 25 who have special needs.

The number of fields within the database will need to be extended to take account of Pilot 1 and Pilot 6 requirements.

3 Pilot 1 Web Application

There is a need for staff within Connexions and partner organisations to share data on clients to fulfil the "one stop shop" approach that we are being asked to implement by central government.

As previously mentioned, it has been agreed that a single electronic signposting system would appear to be the most acceptable approach.

Why not give partners access to Aspire?

There are two main reasons for this as follows:

- (i) Partners would need to gain access to our WAN, which would not be easy as insufficient have the appropriate infrastructure.
- (ii) The security within Aspire would require major changes to limit the access needs of partners.

What other benefits are there to using a Web Application?

- (i) All except one of the partners already has access to the Internet, thereby having the infrastructure required to run a web application.
- (ii) Ideas Integration who maintain Aspire, have already written a simple web version of Aspire that could easily be modified to meet our needs.
- (iii) Security will high but be easy to monitor and maintain.

Pilot 6 Web Application

Unlike the Pilot 1 Web Application, the use of Pilot 6 is likely to grow and become an intrinsic part of the Connexions operation. Therefore as Pilot 6 has a need to view and update data within Aspire it makes sense to develop the two products in a cohesive manner.

Also a Download / Upload routine would appear to be a prerequisite as there is a high likelihood that the system will be used while out of the office.

DRAFT CLIENT CONSENT FORM

The Connexions Service

The Connexions Service is here to help you by giving you information, guidance, advice and support.

In order to do this we may need to share information with schools, colleges, employers, training organisations and our other partners. We also provide statistics to the Department for Education and Employment.

The Connexions Service in Lincolnshire and Rutland uses a database to record all the work we carry out with our clients. All our staff can use the information in order to help you.

The information we record is:

- Name, Address and Date of Birth
- When you have seen us or spoken to us and what notes our adviser made
- What you are currently doing
- What you are looking for
- Your qualifications
- The work and training you have done in the past
- Details of benefits relevant to your situation including those accessed through contact with the Connexions Service

Shared Information

In order to improve support for young people a range of agencies have agreed to share a limited amount of information on a shared database. This means that if you are receiving advice or support from two or more agencies, they will be able to work together with your agreement to help you.

Please note that subject to your consent our partners may be asked to supply similar basic information about you to this database and that our partners will all have access to this basic information held on you on our database

At this moment the current list of partners is: Connexions.....

An up to date list of partners is held on our web site, along with a copy of our data sharing protocol

Or telephone our Learning Line on.....and we can send you a copy

Your information will only be used in the ways described in this leaflet and is kept under the rules of the Data Protection Act.

Equal Opportunities Monitoring Data

This data is for Connexions purposes only

We collect this data for:

- Monitoring purposes
- To make sure that all clients are able to get the information, guidance, advice and support that they are entitled to from the Connexions Service

Please tick whichever box describes your ethnic origin most accurately

Please tick any of the following disability codes that you feel apply to you

Declaration:

I consent to my information being used in the ways described in parts one two and three above and my consent is deemed to continue unless at any point I withdraw my consent.

Name:

Signature:

Date:

Address:

Date of Birth:

Please Note:

You have a right to see the information that we have about you
You have the right to withdraw your consent at any time