

Data and Information Management Protocol

1. General Principles

Staff in the Centre team, consortium partners and other contracted agencies working for the C4EO Centre (hereafter simply termed '*C4EO staff*') will work to the best professional standards and highest ethical principles.

Particular care is needed when securing, using, storing and sharing data and information, especially if this relates to named data from institutions or individuals.

In securing and managing data and information, C4EO staff need to:

- respect the privacy of individuals and institutions
- be sensitive, polite and helpful in their dealings with others
- be mindful of cultural, religious, gender and other relevant differences in the planning, conduct and reporting of their work
- protect the confidentiality of the data or information collected
- produce findings and judgements based on sound evidence
- disseminate Centre outputs and findings openly, honestly and in accessible forms to relevant audiences for them to use in improving outcomes for children and young people.

The paragraphs below set out a series of protocols to which C4EO staff need to work in order to comply with the Data Protection Act and to adhere to best practice in information and data usage and sharing.

2. Securing Data and Information

C4EO staff will advise those from whom they are seeking to acquire data or information of the purposes for which it is to be used – whether it is named or not. They will only use such data or information for the declared purposes; any proposed change of usage will need to be authorised by those supplying the information.

2.1 Named and Sensitive Data

The 1998 Data Protection Act, under which NCB - and hence the C4EO Centre - is formally registered, protects the rights of individuals and institutions with regard to the use of named data. All C4EO staff, partners and

agencies are required – as part of their contracts with NCB - to conform to the provisions of this Act. A copy of the Act and NCB's registration is available upon request from NCB.

Before securing named information about, or views from, children under 18 or vulnerable adults, permission must be sought from the parent, legal guardian or head of education or training institution or his/her representative. Where this is not forthcoming, the child or vulnerable adult needs to be omitted from the C4EO activity.

In the case of sensitive personal data, the explicit written consent of the data subject or legal guardian must be sought. '*Sensitive data*' is data which has background characteristics of individuals attached such as ethnic background, age and gender.

In collecting named information, it needs to be made clear that the C4EO Centre (for which NCB is the accountable body) is the data controller, and that the information is to be used solely for the stated objectives of the Centre.

Ethical and confidentiality issues in relation to the safety of young people will conform to NCB's Code of Practice. Any information about specific young people and their families obtained by C4EO staff or contractors will be anonymised and returned to the relevant organisation or shredded. It will not be referred to in C4EO publications unless permission is sought from the relevant organisation and it is suitably disguised to protect the young person and their family's confidentiality.

3. Storing and Holding C4EO Data and Information

As stated in C4EO contracts with NCB, neither C4EO staff nor any person connected to them shall divulge to any unauthorised person or persons, information of a confidential nature relating to the programme of work of the C4EO or those involved without the consent of all the parties concerned. It is the responsibility of all parties to ensure that confidential documents are clearly marked as such.

Centre staff and partners should ensure that C4EO data and information not in the public domain, held either in hard copy or electronically, is stored with appropriate levels of security and confidentiality. Electronic documents should be password protected, with access limited to designated staff legitimately working on C4EO activities.

4. Releasing and Sharing C4EO Data and Information

C4EO staff will not release the names of institutions participating in its activities to the sponsor (DCSF) or to other third parties, except where permission has been given by the head(s) of institution or their representative(s).

C4EO staff may, however, share the names of participating institutions and other confidential information with consortium partners for the purposes of meeting the Centre's objectives. Such information sharing should adopt the 'sending' procedures set out in Section 5.

Data/information gathered by C4EO staff or contractors that identifies institutions or individuals is held in confidence and will not be released to people outside the consortium (including the sponsor) without the consent of the individual(s) and/or the institution(s) concerned having first been secured.

Similarly, data that identifies individuals or institutions, supplied to the C4EO Centre by a legitimate third party, will not be released to anyone outside of the consortium, other than to that third party.

4.1 Sharing Library Resources

C4EO partners will share library references and publications as far as they can, although existing electronic database and journal licences often prevent staff from sharing such information as widely as they would wish. Borrowing resources will be carried out through the British Library, or by special arrangements between partner library and information services.

The C4EO library and information services group will prepare a copyright statement for the Centre (to be appended to this protocol), and this will be sent out with any library resources that are shared between partners.

5. Sending Data or Information

Routine, non-confidential information (relating to the work and interactions of the Centre) can be sent by e-mail, post, CD or via the C4EO intranet. Care should be taken to ensure that the receivers are legitimate C4EO staff, partners, contractors or contacts.

Care should be taken when circulating non-public contact lists or other material with named or identifying information that appropriate permissions from individuals or institutions have been received beforehand. Such material should be sent in a secure way around the consortium, using the C4EO intranet or password protected e-mails.

Extra special care should be taken when sending numerical data and datasets via post, courier or e-mail, as follows:

- Numerical, anonymised datasets (that have no identifying information) should be sent by e-mail or CD. For both formats, the data should be password protected and encrypted, with the password sent separately and a received and read e-mail received
- If datasets are not anonymised, they must be sent on CD and sent by either recorded delivery or secure courier service. Such data must be

password protected and encrypted, with the password sent separately. Recipients must confirm receipt of the data and a record of that confirmation kept on file.

6. Publishing Centre Material and Outputs

C4EO Centre outputs and publications will not identify any institution or individual without the consent of the head of that institution (or his/her representative) or the individual (or legal guardian for children under 18 and vulnerable adults).