ANNEXES: SUMMARY

ANNEX 1: MODEL PRIVACY IMPACT ASSESSMENT (PIA)

As stated in the document below: "The purpose of a PIA (Privacy Impact Assessment) is to demonstrate that programme managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or programme. This involves making certain that privacy protections are built into the system from the initiation of development, not after the fact, when they can be far more costly or could affect the viability of the project."

Additional approaches to identifying, managing and documenting risks to privacy exist. One such example is the Privacy Impact Assessment Framework (PIAF). PIAF is a European Commission co-funded project that aimed to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and to the processing of personal data.

The PIAF provides: ' *…a process that focuses on identifying the impacts on privacy of any new project, technology, service or programme and, in consultation with stakeholders, taking remedial actions to avoid or mitigate any risks. The process should start when a project is in the early planning stages, when there is still an opportunity to influence the project's design or outcome. The process should carry on throughout the project's life. New risks may emerge as the project progresses, and they should be assessed whenever they become apparent.*'

Wright D and Wadhwa K 2012 'A step by step guide to privacy impact assessment' [4]

ANNEX 2: MODEL CLAUSES FOR CONTRACTS WITH THIRD PARTIES

A: BENEFICIARY NOTICE AND CONSENT (PLAIN LANGUAGE TEMPLATE)

B: AID AGENCY AND E-TRANSFER SERVICE PROVIDER

Please note that the clauses represent a recommended standard but will need to be amended by the relevant Agency (i) to accommodate variations in terminology and naming conventions in the data protection laws applicable to the countries concerned; or (ii) to adopt higher standards of data protection; or (iii) to accommodate specificities in the engagement between the particular Agency (Data Controller) and Data Processor.

CaLP attempts to provide the practitioner with a starting point in the development of clauses that are in line with the Principles and Operational Standards outlined in this document.

Additional clauses will be made available on the CaLP website www.cashlearning.org