Liquidlogic electronic Common Assessment Framework (eCAF)

Acceptable Use Policy & Data Processing Procedure

Summary Sheet

Protective marking:	Unclassified
Ref	**eCAF-AUP-1**
Purpose	Identifies key system usage behaviour for access to eCAF and specifies data processing requirements to be understood and adhered to by non-Council staff in the processing of the Council;s eCAF data Supplements existing Council-wide Acceptable Use Policies and Procedures that must be adhered to by **all** individuals accessing eCAF.
Partners	N/A
Date agreement came into force	August 2014
Date of Review	August 2015
Owner	Sefton Council (Early Intervention & Prevention)
Location of original	Data Protection Officer, Sefton Council, Business Intelligence & Performance Team, 7th floor Merton House, Bootle

Version Control

Version	Date	Amendments / Comments	Authorisation
1.0	August 2014	Initial Draft	N/A
1.1	September 2014	Revised	N/A
2.0	January 2015	Revised following discussion with BIT	N/A

Liquidlogic electronic Common Assessment Framework (eCAF)
Acceptable Use Policy & Data Processing Procedure

Introduction

Access to Sefton Council's Liquidlogic eCAF system and associated electronic and paper information must be adequately protected for business and privacy reasons.

This policy applies to any person – whether data processing on behalf of the council or a relevant Sefton Council employee - that requires access to Sefton Council's eCAF system.

User Access Control

Assess to eCAF will only be granted upon completion of the following training courses:

- CAF Awareness Training
- CAF Assessor Training
- eCAF online e-learning programme

Upon completion of the CAF Assessor Training, access will be given to the eCAF online e-learning programme. Once the e-learning programme has been successfully completed, details will be forwarded to Arvato who will then provide access to the eCAF system.

Access to eCAF will only be granted upon successful completion of the on line e-learning programme.

Each user will be allocated the appropriate level of access rights and permissions to eCAF. These access rights will be commensurate with the tasks they are expected to perform.

User's access rights must be reviewed at regular intervals by the authorising person to ensure that the appropriate rights are still allocated.

When an employee leaves the post relevant to their eCAF connection, their access to computer systems and data must be suspended on the employee's last working day at the close of business.

It is the responsibility of the line manager or supervisor of the leaving member of staff to inform Sefton Council and/or the arvato helpdesk to request the suspension of the system access rights.

User Responsibilities

Each user will be allocated a unique login, initial password, and security questions that must be changed as part of the first login process.

Users must ensure that their login, password, and security question answers are not shared with, or disclosed to, any other user of the system. Passwords must not be displayed on or near the workstations being used and must not be written down. Failure to maintain secure passwords in accordance with this policy may result in disciplinary action being taken against you.

In the case of third party suppliers or consultants, non-conformance will result in the immediate removal of access to the system. If damage or compromise of Sefton ICT systems or data results, Sefton Council will consider legal action against the third party.

It is a user's responsibility to prevent unauthorised access to Council systems by:

- Ensuring that unattended PC's are locked or logged out
- Leaving nothing on display that may contain access information such as login names and passwords
- Informing Sefton Council and/or Arvato of any changes to their current role
- Ensuring their access to client records is in accordance with their current roles and responsibilities and follows the appropriate policies and procedures for access

You must not use the eCAF database to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for immediate disciplinary action and any criminal activity will be reported to the police.

You must not use the eCAF database for commercial gain. This includes, but is not limited to: unsolicited marketing, advertising and selling goods or services.

You must not download or extract data from within the system unless it is explicitly within your job role to do so. Any downloading or data extraction must conform to the existing data handling, protection, sharing, and encryption policies of Sefton Council.

You must only access data subject records with which you have a legitimate professional relationship. There are no exceptions to this principle as it is a major concern for data protection breaches. Disciplinary procedures may be taken with those who are assessed as deliberately viewing records to which they would not normally have access as a result of their job. This includes, but is not restricted to, viewing the records of family members, former spouses, neighbours, or other records where the data subject may be known to the user.

Where access is inadvertently made to an inappropriate record this should be reported to your line manager and recorded.

Where access is required to records that could be deemed inappropriate but where there is an operational imperative to work on the record then the appropriateness of access should be discussed with your line manager and a record should be kept of the reason for access.

Users should note that system use is audited centrally to ensure no inappropriate access of data subject information and each database user can review who else has been viewing data subjects' files which provides local auditing of record access.

If data subject identifiable information is visible to other people with whom you are working, it is your responsibility to make sure that those people have a valid relationship with the data subject.

You must adhere to local and national privacy and confidentiality standards such as:

- Data Protection Act 1998
- Caldicott Report 1999

Data Processing

As an individual Data Processor you will comply with all legal requirements in relation to the management and processing of any data received or directly accessed through use of the eCAF system.

As the Data Processor you warrant that:

- You will not allow shared or accessed data to be stored in an insecure environment.
- The data you access will not be shared or used for any purpose other than that specified by Sefton Council as the Data Controller
- No electronic version of the data will be removed or copied from computers to portable computer or portable storage devices (including, but not limited to, CD, DVD, memory sticks or portable hard drive) without the use of secure encryption to a standard acceptable to Sefton Council as the Data Controller.
- you will not further process this data for any purpose other than those identified in this agreement unless directed by Sefton Council as the Data Controller
- On completion of the work, all copies of the data will be securely destroyed in a manner and to a standard acceptable to Sefton Council as the Data Controller

Training, Supervision, & Audit

As the Data Processor you confirm:

- You have appropriate levels of training and understanding either separately or as part of continuing professional development covering:
    1. Sefton's eCAF Acceptable Use Policy & Data Processing Procedure and its operation
    2. The Information Sharing Agreement and its operation
    3. Data Protection and Information Management Principles as it applies to handling data
- You have been assessed for reliability in line with the employer's requirements for the role (for example Disclosure & Barring Scheme checks where appropriate)

Data to be Processed

As identified in the Information Sharing Agreement with your organisation.

Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

Where you are accessing the system as a third party as covered by an information sharing agreement you may also be subject to the disciplinary procedures of your own organisation.