TAKING PERSONAL DATA OFF COUNCIL PREMISES POLICY

Denbighshire County Council (DCC) officers may need to take personal data out of the office. The purpose of this policy is to set out the steps to be followed by officers when taking personal data offsite, for example, to conduct home visits, attend meetings, panels or court, or to work from home. Following this policy will help to reduce the risk of a security breach involving personal data and any subsequent fine.

For ease of reference, throughout this policy, the term 'personal data' includes 'sensitive personal data'.

Circumstances in which personal data can be taken off site

In order to ensure the security of the information, and the safety and welfare of the service user, the following points must be complied with:

- Personal data should only be taken off DCC premises when absolutely necessary and for the shortest possible time.
- Only the absolute minimum amount of personal data is to be taken out of the office. Relevant papers should be removed from the file where this is possible rather than the entire file being taken.
- Where a substantial amount of personal data is to be taken off site, then the officer must have approval from his/her line manager.
- Preference should always be given to accessing personal data remotely using digital means rather than taking data off site in other formats, such as on paper. Digital access should be done through CAG access the Council's Systems.
- Where notes have been taken by an officer working off site, they must be written up onto the appropriate Council System as soon as reasonably possible. Once they have been formally written up, the informal notes should be securely destroyed. Please note that all concurrent notes taken during investigation, assessment or proceedings, should be securely destroyed upon completion of proceedings or once a case is closed.

Means and mode of transport

- Alternative secure digital methods should be considered for situations where accessing the Council's Systems remotely is not possible e.g. encrypted memory sticks or DCC issued laptops and IPads.
- Paper records must be transported in a receptacle, which fully closes (locks / zips / clips shut), and which is made of a non-transparent material.

- When transporting paper records on public transport, for example, by bus or train then the records must be kept with the officer and not placed on luggage racks.

- When transporting paper records by a vehicle then these should be stored out of sight in a locked car boot. This also applies to electronic media such as laptops. Officers should remain vigilant when opening car doors, boots, etc. to ensure that records do not fall out of the vehicle or blow away.

- Personal data should not be reviewed or discussed by officers in places where it could be seen, or conversations overheard, by a member of public, for example, on public transport or in cafes.

Working from home

- Care must be taken when working from home to ensure that personal data is not visible to other members of the household and that work related conversations are held out of earshot of other household members.

- Personal data must be stored in the officer's home in a safe place, which is out of sight.

- Personal data must be returned to DCC premises the next time the officer is due in the office.

Information security incidents

If an officer becomes aware of any information security related incident, then the officer must immediately inform his or her line manager who should in turn inform the ICT Servicedesk. DCC's Information Security Breach Procedure will then be followed.

Policy statement

This policy is underpinned by DCC's Information Security Policy.

Failure to adhere to this procedure may be regarded as serious and any breach may render an employee liable to action under the Council's Disciplinary Procedure, which may include dismissal.