

Policy: Physical Security of Data

SUMMARY OF PRINCIPLES:

- *Cofnod will ensure that data in its care is protected from alteration, damage, loss, theft and unauthorised copying.*

1. POLICY STATEMENT

- 1.1. The information and data held at Cofnod is its main asset and in some cases may be irreplaceable. Where Cofnod is the nominated custodian of a dataset it is responsible for managing the data properly *and* ensuring it is physically secure.
- 1.2. The replacement of much of the data held at Cofnod is likely to be extremely costly or even impossible (in the case of lone copies of paper records). Cofnod has an obligation to data owners to ensure that their data is safe and secure whilst in the care of Cofnod.
- 1.3. Cofnod will take a range of physical and procedural steps in order to:
 - Protect against physical damage to data by fire, floods, wear and tear and vandalism.
 - Prevent the alteration or deletion of original data.
 - Protect against theft or unauthorised copying of paper and computerised data.
 - Prevent the corruption of computerised data.
- 1.4. This policy is implemented through the following 'statement of procedure'. Please note that this policy deals with physical aspects of data security and not issues relating to the unauthorised use of information supplied to users (*see Cofnod's Policy on 'Data Sourcing, Management and Use'*).

2. STATEMENT OF PROCEDURE

- 2.1. Cofnod is currently housed in offices managed by Gwynedd County Council. These offices benefit from a high level of security. The main entrance to the building has a manned reception and is only open to the public during normal working hours (9 till 5, Monday to Friday). Outside these hours the building is only accessible to named key holders using an electronic key fob system. This key fob allows access to the outside doors and Cofnod's corridor, but only Cofnod's named key fob holders and the master key fob holder (who manages the building on behalf of Gwynedd CC) can access Cofnod's Office Unit. Electronic records of the use of the key fobs are kept and can be requested if required. The building has an internal and external CCTV camera network. The shared areas are fire and security alarmed, whilst Cofnod has its own fire and intruder alarm which dials to a monitoring centre if triggered. When the office is unoccupied, all windows are closed, the door is locked and the intruder alarm is activated.
- 2.2. Offices have been subject to fire safety inspections and an all-purpose fire extinguisher is kept on the premises. This will be regularly serviced or replaced as appropriate. Cofnod has a designated fire marshal and all staff are aware of evacuation procedures in the event of a fire. This does not however include the removal of any equipment which stores data or any paper records as safety of life is the first priority in these circumstances.

- 2.3. The Cofnod offices are not prone to flooding. Water damage is still a possibility if leaks or dampness should arise. Should any such occurrences be noted, data will be removed from the vicinity and remedial works will be undertaken as soon as possible.
- 2.4. Back-up copies are made of all incoming electronic data as it arrives at Cofnod. These are catalogued in Cofnod's Administration Database Orca and stored on Cofnod's Microsoft Sharepoint. If original paper records are held at Cofnod, these will be stored appropriately and notes on their storage are kept in Orca.
- 2.5. Paper records will not be marked or defaced in any way which masks the details of the original record. Where paper records are marked (e.g. stamped to show they have been computerised) marks will only be made well away from the text of the record.
- 2.6. Full and direct access to Cofnod databases is restricted to Cofnod staff. All internal computer systems are password protected and staff are required to logoff or lock their work station when they are not in the office. Furthermore access to Cofnod's Administration Database Orca, cataloguing the location of original data, is also password protected, as are any methods of accessing the Cofnod Species database.
- 2.7. Computer systems will be maintained to the highest standards including regularly updated anti-virus and firewall software to prevent data theft or corruption. All incoming files will be scanned for viruses prior to their use.
- 2.8. All essential computer files are held on a on a Microsoft Azure Cloud Server and are subject to regular back-ups. All data are backed up onto cloud storage solutions and incremental backups are made daily. The back-up system has been fully tested to ensure that systems can be easily restored in the event of data loss or corruption.
- 2.9. Procedures for ensuring continuity of service are set out in Cofnod's Business Continuity Plan and for ensuring the continuity of its systems are set out in Cofnod's Disaster Recovery Plan.