



Connevens Limited Data Management & Security Policy

Connevens Limited depends on Information and Communications Technology (ICT) systems to operate. Security of these systems and the data they hold, and of the hardware and networks on which they operate is necessary both to honour our obligations to providers of data (customers, suppliers, staff etc) as registered under the Data Protection Act, and to protect the company's systems and data from accidental or deliberate damage, loss or corruption. This policy statement is intended to effect implementation of the overall information security policy in respect of data held in ICT systems. All staff have a responsibility to comply with the Connevens policy on confidentiality of data and to comply with this statement of policy on data security.

The key points of our strategy to achieve this are as follows:

- Data is owned by Connevens Limited and is the responsibility of the Management Team, who are accountable for the security of that data and determine the standards of confidentiality that are to apply.
- All personal data is maintained for the purpose defined within the notification under the Data Protection Act
- Access to our data stores is limited to those needing such access to do their job and the system design facilitates such access. Each member of staff with such access is personally responsible for maintaining the confidentiality of the data to which he/she has access.
- Data whether in electronic or physical form is subject to physical security control appropriate to its nature. Physical access is determined on the same basis as data access unless there are over-riding security reasons for doing otherwise.
- General facilities such as e-mail and conferencing are provided for business purposes and the data generated by these is treated as belonging to the company.
- Data may be held on central servers, the company portal, personal workstations, portable devices such as laptop computers and smartphones, and other removable media such as floppy/ZIP disks, readable CD's/DVD's and USB flash drives. Data held in central locations are the responsibility of the IT Supervisor. They will be responsible on behalf of Data Owners for the security of data deposited on these servers. Security of data held on personal workstations, portable storage devices or on associated removable magnetic media (including video recorders) is the responsibility of the individual member of staff who operates the equipment.
- Responsibility for the security of the Connevens Limited network (including software, hardware and general services) rests with the IT Supervisor on behalf of the Managing Director. This responsibility is limited to the security of data in transit and ends when the data is delivered to its destination.
- System specifications define the requirements for back up copies of programmes and data appropriate to the requirements of the system as determined by the IT Supervisor, institutional and legal requirements.

- Contingency disaster plans are required for core systems and are authorised by the Business Recovery Team (See Business Continuity Management Plan).
- All staff have a personal responsibility to safeguard the integrity and confidentiality of the company's systems, data and physical facilities. Line management is responsible for the application of the data security policy for matters under their control. They must ensure that all staff are aware and comply with the policy. Breaches in security could lead to disciplinary action.

To ensure we meet these commitments we will review our data security policy regularly.

A handwritten signature in black ink, appearing to read 'David Evans', with a long horizontal flourish extending to the right.

David Evans
Managing Director
January 2016