General Data Protection Regulations (GDPR)

We are committed to compliance with personal data laws and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with GDPR.

Dorset County Council is working with their partners, and suppliers to obtain evidence of their compliance.

Dorset County Council takes data protection very seriously. During the course of the contract, we will be mindful of the fundamental data protection principles, to ensure that unless an exemption applies, the customer's data is:

1. Fairly and lawfully and transparently processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Secure
7. Be accountable and able to demonstrate compliance

Our security policy includes obligations to ensure that:

- Casual passers-by cannot read information off screens or records left visible on desks
- Passwords are known only to authorised people and changed regularly
- personal information is disposed of securely
- We authenticate the identity of a person to whom personal information is to be disclosed, prior to disclosure
- We securely transmit and receive personal information, especially faxes
- We do not discuss personal information in public places where we may be overheard

We are well equipped to comply with the legislation covering the use, storage and retention of electronic and hard copy documents. Our workforce includes a Data Protection Officer who works as part of the Records Management Unit (RMU), and a named ICT Security manager for each system. The Council has a notification with the Information Commissioner under the Data Protection Act which is reviewed and maintained by the Council's Data Protection Officer.

The RMU provides our policies, training and guidance on data protection and freedom of information, and our secure physical records storage facilities. The corporate ICT Security Group provides the System Access Policy. Physical access control to the building is managed by ID badge access.

The staff code of conduct requires employees to properly protect sensitive, confidential or restricted information. Training available to all staff includes classroom sessions and online e-learning courses for Data Protection and Freedom of Information, Information Governance, Information Security, DCC Information and Data Security Policy and Standards within which employees are made aware of their responsibilities under the Data Protection and Computer Misuse Acts and usage of the Council's Internet and e-mail facilities. Lockable storage is provided and a clear desk policy is in place to ensure the confidentiality of paper records.

We comply with a data retention schedule agreed between HR/Payroll and our Data Protection Officer based on pension regulations, legislation and the Records Management Society of Great Britain. Our records management unit retains historical information and the schedule, and on an annual basis informs us of the records they believe should be destroyed confidentially. Unless there are extenuating circumstances, such as an historical police investigation data is securely destroyed.

We will also be mindful of the rights to privacy that people have, particularly under the Human Rights Act 1998 and the Common Law Duty of Confidentiality. Any requests under 'Subject Access Rights' will be referred to the customer for further guidance, being mindful of the legal requirement to provide the information within 40 calendar days.

As a Data Processor we will inform you of a personal data breach “without undue delay” after becoming aware of it.

At the end of the contract, we will only provide information that is agreed is required to administer the records, and will ensure that data provided is always transmitted, transported or transferred in a secured manner. The customer will need to be satisfied that the provision of personal information relating to their employee’s pay and pension records has followed GDPR regarding disclosure, and has the relevant consent in place