Duxford Parish Council

DATA PROTECTION POLICY

As adopted by Duxford Parish Council on 10th August 2017.

In the course of your work you may come into contact with or use confidential information about employees, clients, customers and suppliers, for example their names and home addresses.
The Data Protection Act 1998 contains principles affecting employees' and other personal records.
Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure you do not breach the Act.
If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Company's Data Protection Officer. Contact your Line Manager for further information.
You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

The data protection principles

There are eight data protection principles that are central to the Act. The Company and all its employees must comply with these principles at all times in their information-handling practices.
In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act.

Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

- Race or ethnic origin.
- Political opinions and trade union membership.
- Religious or other beliefs.
- Physical or mental health condition.
- Sexual life.
- Criminal offences, both committed and alleged.

2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.
3. Adequate, relevant and not excessive. The Company will review personnel files on a regular basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.
4. Accurate and kept up-to-date. If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be held responsible for any errors unless you have notified the Company of the relevant change.
5. Not kept for longer than is necessary. The Company will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data that the Company decides it does not need to hold for a period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.
6. Processed in accordance with the rights of employees under the Act.
7. Secure. Technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and

against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored in locked filing cabinets.
Only authorised employees are permitted to have access to these files. Files must not be removed from their normal place of storage without good reason. Personal data stored on diskettes or other removable media must be kept in locked filing cabinets. Personal data held on computer must be stored confidentially by means of password protection, encryption or coding and again only authorised employees are permitted to have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.
8. Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

Your consent to personal information being held

The Company holds personal data about you and your consent to the Company processing your personal data is a condition of your employment. Therefore, by agreeing to your contract of employment, you also agree to your personal data being held and processed. The Company also holds limited sensitive personal data about its employees and, by signing your contract of employment, you give your explicit consent to the Company's holding and processing that data, for example sickness absence records, health needs and equal opportunities monitoring data.

Your right to access personal information

Under the provisions of the Act, you have the right on request to receive a copy of the personal data that the Company holds about you, including your personnel file to the extent that it forms part of a relevant filing system, and to demand that any inaccurate data be corrected or removed. You have the right on request:

- To be told by the Company whether and for what purpose personal data about you is being processed.
- To be given a description of the personal data and the recipients to whom it may be disclosed.

- To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the personal data.
- To be informed of the logic involved in computerised decision-making.

Upon request, the Company will provide you with a written statement regarding the personal data held about you. This will state all the types of personal data the Company holds and processes about you and the reasons for which the data is processed. If you wish to access a copy of any personal data being held about you, you must make a written request for this and the Company reserves the right to charge you a fee of up to £10 per request. To make a request, please apply to the Company's Data Protection Officer.

If you wish to make a complaint that these rules are not being followed in respect of personal data the Company holds about you, you should raise the matter with the Company's Data Protection Officer. If the matter is not resolved to your satisfaction, it may then be raised as a formal grievance under the Company's grievance procedure.

Your obligations in relation to personal information

You should ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject himself or herself. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given his or her explicit consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another employee, you should forward this to the Company's Data

Protection Officer, who will be responsible for dealing with such requests.

- Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected.
- Compliance with the Act is your responsibility. If you have any questions or concerns about the interpretation of these rules, you should take this up with the Company's Data Protection Officer.

In this organisation, the name of the Data Protection Officer is:

The Parish Clerk