Bugthorpe and Kirby Underdale Parish Council
Data Protection Policy

This policy was adopted by Bugthorpe and Kirkby Underdale Parish Council ('the Council') on 11 March 2019.

1. General Information and statement

Data Controller: Bugthorpe and Kirby Underdale Parish Council

Address: c/o Estate Office
Bugthorpe
York
YO41 1QG

Daytime telephone: 01759 368219

Email: dlord "at" halifaxestates.co.uk

Data Processor: The Clerk, David Lord

Bugthorpe and Kirkby Underdale Parish Council needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry out its work. This personal information must be collected and dealt with appropriately – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this under the General Data Protection Regulations 2018.

The following list of definitions of the technical terms is intended to aid understanding of this policy.
Data Controller – The person who (either alone or with others) decides what personal information the Council will hold and how it will be held or used.
General Data Protection Regulations 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.
Data Protection Officer – The person(s) responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998
Data Subject/Service User – The individual whose personal information is being held or processed by the Council (for example: a client, an employee, a supporter)
'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data (* See definition)
Informed consent: Is consent given when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data, and then gives their consent in writing.
Notification – Notifying the Information Commissioner about the data processing activities of the Council, as certain activities may be exempt from notification.
Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.
Processing – means collecting, amending, handling, storing or disclosing personal information
Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within the Council.
Sensitive data – means data about:
• Racial or ethnic origin
• Political opinions
• Religious or similar beliefs

• Trade union membership
• Physical or mental health
• Sexual life
• Criminal record
• Criminal proceedings relating to a data subject's offences

Data Controller

Bugthorpe and Kirby Underdale Parish Council is the Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Disclosure

The Council may share data with other agencies such as the local authority, funding bodies and other voluntary agencies but only with the consent of the individual.

The Data Subject will be made aware in all circumstances how and with whom their information will be shared. There are circumstances where the law allows the Council to disclose data (including sensitive data) without the data subject's consent. These are:
1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion.

The Council regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.
Bugthorpe and Kirby Underdale Parish Council intends to ensure that personal information is treated lawfully and correctly. To this end, the Council will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulations 2018.

Specifically, the Principles require that personal information:
1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The Council will, through appropriate management, strict application of criteria and controls:
i. Observe fully conditions regarding the fair collection and use of information,
ii. Meet its legal obligations to specify the purposes for which information is used,
iii. Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
iv. Ensure the quality of information used,

v. Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
• The right to be informed that processing is being undertaken,
• The right of access to one's personal information
• The right to prevent processing in certain circumstances and
• The right to correct, rectify, block or erase information which is regarded as wrong information,
vi. Take appropriate technical and organisational security measures to safeguard personal information,
vii. Ensure that personal information is not transferred abroad without suitable safeguards,
viii. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
ix. Set out clear procedures for responding to requests for information.

Data collection

The Council will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, the Council will ensure that the Data Subject:
• Clearly understands why the information is needed
• Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
• Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
• Has received sufficient information on why their data is needed and how it will be used

For children under the age of 13, consent will be sought from a parent/guardian.

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers (see guidelines below).

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is the Council's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data access and accuracy

All Data Subjects have the right to access the information the Council holds about them. The Council will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes. When a Data Subject requests some or all of their personal data from the Council, he or she will be advised to do so in writing if the request is verbal. The Council will respond within twenty working days, either providing the data requested, or advising the Data Subject when it will be made available, or providing a legal reason why the request cannot be fulfilled. The Council will verify the identity of the requestor to ensure that a data breach does not occur and follow the NALC's GDPR Toolkit guidelines to fulfilling an Subject Access Request.

In addition**,** the Council will ensure that:
• The Clerk, as Data Processor, manages compliance with Data Protection,
• Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
• Everyone processing personal information is appropriately trained to do so,
• Everyone processing personal information is appropriately supervised,
• Anybody wanting to make enquiries about handling personal information knows what to do,
• It deals promptly and courteously with any enquiries about handling personal information,
• It describes clearly how it handles personal information,
• It will regularly review and audit the ways it hold, manage and use personal information
• It regularly assesses and evaluates its methods and performance in relation to handling personal information
• All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

Data breaches

In the event of discovery of a data breach which might cause harm to a Data Subject, the Council will inform the Information Commissioner's Office within 72 hours, and if appropriate, will inform the Data Subject(s) affected.

The Council will review how the breach occurred and take action to help prevent future breaches (see guidelines below).

Guidelines for storage of personal data

The following guidelines apply to all devices used to store electronic or hard copy personal data for the Council, whether or not they are owned by the Council and whichever authorised personnel are using the device:

Manual records

(i) All papers should be securely locked away when not in use to prevent other people from inadvertently gaining access.
(ii) Filing cabinets must be locked outside of normal working hours and keys must be held securely by nominated personnel.

Computerised records

(i) Access should be controlled by unique password and passwords should be changed on a regular basis. Passwords should not be easy to guess;
(ii) Passwords and access controls should be kept secure when not in use e.g. passwords should not be written down and stored in a place that is easy to guess;
(iii) Personal information should not be left displayed on the screen when unattended;
(iv) Devices should be turned off or locked when not in use;
(v) Removable storage devices such as USB sticks should be filed away securely;
(vi) Workspace containing a computer or other device containing data should be locked when not in use.
(vii) Particular care should be taken to ensure the security of personal data on portable devices such as a laptop or tablet.

Guidelines for preventing breaches of personal data

A data breach is a breach of security leading to ‘accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data’. If there is minimal risk of harm to an individual (for example because some low risk data such as an email address has been inadvertently

released) then the breach would not need to be reported. Where there is a risk of harm to a Data Subject, the Information Commissioner's Office must be informed within 72 hours. For example, unauthorised access to data that could be used to steal someone's identity, such as their banking data, must be reported.

Examples of personal data breaches and steps to avoid them include:

- Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient - Check thoroughly before clicking 'send'.
- The wrong people being copied in to emails and attachments – Use BCC (Blind Carbon Copy) where necessary.
- Lost memory sticks which contain unencrypted personal data – Store such devices securely and, if used away from the office, encrypt the data.
- Malware (IT) attach – Ensure up to date anti-virus software is in place.
- Equipment theft – Follow the security guidelines.