

Data Protection Policy

Resolved on 3rd December 2018 PC19 92 (iv)
Review December 2020

ICO Registered Number Z7761368

We understand that individuals need to know that their data is collected, why it is processed and whom it is shared with. We will publish this information in our privacy notices on our websites and within any forms or letters we give to individuals.

The information will be:

- concise, transparent, intelligible and easily-accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Right of Access

People have the right to:

- obtain confirmation that their data is being processed
- access their personal data

We follow the Information Commissioner's Office's 'Subject Access Code of Practice' to identify and respond to subject access requests. However, our timeframe is in line with the General Data Protection Regulation:

Information must be provided without delay and at least within one calendar month of receipt of a subject access request. We can extend this period by a further two months for complex or numerous requests (in which case the person must be informed and given an explanation). A calendar month ends on the corresponding date of the next month (e.g. 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (e.g. 31 January to 28 February).

This means that the legal deadline will vary from 28 days to 31 days depending on the month.

Keeping Data Accurate and Up-To-Date

We respect that people have the right to have personal data rectified if it is inaccurate or incomplete and we will respond to a request without delay (at least within one month of receipt). In some circumstances it may be necessary to extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). If we have disclosed the personal data to a data processor (third party) we will inform them of the rectification where possible.

As part of our annual review of our information asset register, we will review the information we process or store to identify when we need to do things like correct inaccurate records. Records management policies, with rules for creating and keeping

records (including emails) will help with this.

If we identify any data accuracy issues, we are committed to communicating lessons learned to staff through ongoing awareness raising and internal training.

Disposing of Personal Data

We will securely dispose of personal data for the following reasons:

- it is no longer required for the purpose for which it was originally collected/processed, or
- when the person withdraws consent
- when the person objects to the processing and there is no overriding legitimate interest for continuing with the processing
- if the data was unlawfully processed
- it has to be erased to comply with a legal obligation

There are occasions when we can refuse to delete personal information; please refer to the ICO web site for guidance.

A retention schedule is included within our information asset register to remind us when to dispose of different categories of data. The schedule will be reviewed annually to ensure that it continues to meet council and statutory requirements.

Restrictions on Data Processing

People have a right to block or restrict the processing of personal data. In these situations, we can store the personal data, but not carrying out any further processing of it. We can retain just enough information about the person to ensure that the restriction is respected in the future.

Processing restrictions to personal data are required in the following circumstances:

- Where a person contests the accuracy of the personal data, we will restrict the processing until we have verified the accuracy of the personal data.
- Where a person has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our business's legitimate grounds override those of the individual.
- When processing is unlawful and the person opposes erasure and requests restriction instead.
- If we no longer need the personal data but the person requires the data to be retained to allow them to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We will inform individuals when we decide to lift a restriction on processing.

Objecting to Processing

We understand that people have the right to object to the following:

- Processing their personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Processing for purposes of scientific/historical research and statistics.

We will stop the processing in response to an objection unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

People can also object to any processing undertaken for direct marketing (including profiling). We will stop processing for direct marketing as soon as we receive an objection. We will inform individuals of their right to object “at the point of first communication” and clearly lay this out in our privacy notices.

Data Portability

If we process data by automated means, people are allowed to receive that personal data, or have it moved, copied or transferred to a business in a safe and secure way. However, this only applies to:

- Automatically-processed data which is also
- Personal data that an individual has provided to us
- Where processing is based on consent, or for the performance of a contract

Where the above conditions apply, the information will be provided without delay and at least within one month of receipt. We can extend this period by a further two months for complex or numerous requests (in which case the individual will be informed and given an explanation). We will provide the personal data in a structured, commonly used and machine-readable format, e.g. XML files.

The information will be provided free of charge and if requested by the individual, we can transmit the data directly to another business where this is technically feasible.

Automated Decision-Making

At this time, the Parish Council does not carry out processing that could be constituted as automated decision-making. Should this change, the council will review this policy to ensure that the required safeguards are put in place to prevent any potentially damaging decisions being taken without human intervention.

Working with Data Processors

We will put a written contract in place with any processors that we work with.

We understand that we are liable for our processors’ compliance with the GDPR and must only appoint processors who can provide ‘sufficient guarantees’ that the requirements of the GDPR will be met and the rights of data subjects protected.

Information Risks

The Parish Clerk has overall responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk-assessing information assets.

If an information risk is identified, the Parish Council will put in place an appropriate action plan to mitigate any risks that are not tolerated or terminated.

Data Protection by Design and Default

We have a general obligation to implement appropriate technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

We will adopt internal policies and implement measures which help the Parish Council to comply with the data protection principles.

Data Protection Impact Assessments (DPIAs)

We do not carry out processing of a nature that requires us to conduct DPIAs. However, if our processing changes to incorporate this, we will introduce them.

Information Security Policy

Our Information Security Policy is contained within our IT policy. This is based on the risks to the personal data that we hold and security measures that are appropriate to our needs.

International Transfers

We are committed to ensuring an adequate level of protection for any personal data processed by others on our behalf that is transferred outside the European Economic Area.

Data Breaches

A data breach is a breach of security leading to the destruction, loss, alternation, unauthorised disclosure of, or access to, personal data.

We have an internal breach reporting procedure to identify, report, manage and resolve any personal data breaches. We will adhere to ICO guidelines to identify which data breaches should be reported to the ICO, and to the individuals affected.

We will maintain records of personal data breaches, whether or not they are notifiable to the ICO.

A notifiable breach will be reported to the ICO within 72 hours of the council becoming aware of it.

Roles and Responsibilities

Overall responsibility for Data Protection compliance lies with the Parish Clerk:

It is the Clerk's responsibility to:

- Inform and advise the council and its officers about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, training any staff and conducting internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, service users, etc).

Procedures

Individual procedures will be put in place for each area of the Parish Council to ensure that data is being correctly processed.

Compliance

Failure to comply with this policy will result in disciplinary action being taken in line with the council's Disciplinary Procedure.

NOTIFICATION TO THE INFORMATION COMMISSIONER

The Information Commissioner maintains a public register of data controllers. The Council is registered as such. The Data Protection Act 1998 /GDPR May 218 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Officer will review the Data Protection Register annually, prior to notification to the Information Commissioner. Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between reviews will be brought to the attention of the Information Officer immediately.