Buildwas Parish Council

Data Subjects Rights -
Policy and Procedure

Introduction

This policy and procedure explains how Buildwas Parish Council will meet the rights of individuals concerning the information it holds about them.

This includes being transparent about the information we hold and how it will be used and shared; telling people what information we have about them and putting right or erasing information which is incorrect or out of date.

Individuals may ask us to restrict the use of their information or to stop using it altogether. There are also rights concerning data portability and using data for automatically making decisions.

Some of these rights depend on why the information is being used and considerations can be complex.

Contents	

Individual Rights of Data Subjects

Buildwas Parish Council's Data Protection Policy sets out the broad organisational and employee requirements with regard to data protection legislation.

This policy explains the rights of individual data subjects whose data the Council may process, and the procedures the Council will follow to ensure those rights are met.

The Rights

Under data protection legislation, a person whose data we hold has a number of rights, these are:

1. **The right to be informed** – being told about the type of information we collect and how we use and look after it

2. **The right of access (Subject Access Requests)** – being given a copy of the personal data we hold about the individual

3. **The right to rectification** – having inaccurate personal data corrected

4. **The right to erase (the right to be forgotten)** – having personal data deleted from records or records deleted entirely

5. **The right to restrict processing** – requiring us to store but not use personal data concerning the individual

6. **The right to data portability** – being provided with an electronic copy of certain records to use for a different purpose

7. **The right to object** – to put a case forward for stopping processing including marketing

8. Rights in relation to **automated decision making and profiling** – to have a human reconsider automated decisions and profiling

The Legislation

This document is based on the requirements of the General Data Protection Regulation; The Data Protection Act 2018; the guidance of the UK Information Commissioner and EU Article 29 Working Party guidance.

The legislation applies to personal information relating to living individuals who can be identified from it. This may be automatically processed information held on the Council's computer systems, as well as information in our structured manual records, such as paper files. It also applies to CCTV recordings and audio tapes.

The Rights in Detail

The following paragraphs explain the rights in detail and how they should be applied.

Right One - The right to be informed

Legislation requires the Council to be transparent over how we use personal data. We have an obligation to provide 'fair processing information'. That means we must clearly explain to people how we will use the personal information with which we are entrusted. We usually do this by providing a public Privacy Notice.

Legislation sets out the information that we should supply and when individuals should be informed. This is determined by whether or not we obtained the personal data directly from individuals. See the table below for further information on this.

The information we supply must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge, except where costs such as printing and posting is requested

The table below summarises the information we should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (the Council) and the council's data protection officer	✓	✓
Purpose of the processing (what we need to do with the data) and the lawful basis for the processing (what we are legally allowed to do with the data)	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data (who we may share the data with – this could be internal departments or partners/agencies)	✓	✓

Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period (how long we will keep the data)	✓	✓
The existence of each right of data subjects	✓	✓
The right to withdraw consent (for processing) at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority (the Information Commissioner)	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

When devising Privacy Notices, Buildwas Parish Council will follow ICO guidance regarding the 'the right to be informed'.

Responsibility for Privacy Notices

It is the responsibility of the council to ensure that they provide adequate information to their residents and service providers regarding the processing of their data.

Support with the production of suitable Privacy Notices can be sought from the Data Protection Advisory Service.

Once finalised, Privacy Notices will usually be published on the Council's website.

Right Two - The right of access (Subject Access Requests)

Individuals have the right to access their personal data and supplementary information. This allows individuals to be aware of and verify the lawfulness of the way in which their data is being used.

Most commonly, individuals simply want to be given a copy of the information we hold about them. However, under data protection legislation, individuals also have the right to obtain:

- confirmation that their data is being processed;
- other supplementary information (similar to the information that should be provided in a privacy notice – see above)

This is known as a Subject Access Requests (SAR). A request must be made in writing – although we have a standard form for customers to use, they are not obliged to do so.

Charging for information

We must provide a copy of the information free of charge, with the exception that we can charge a 'reasonable fee' when a request is 'manifestly unfounded or excessive', particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information, such as for printing and posting, and in cases where the information takes many administrative hours to collect.

Time constraints

Information must be provided without delay and at the latest within:

- one month of receipt for standard requests
- three months of receipt where requests are complex or numerous BUT ONLY if we inform the individual within one month of the receipt of the request and explain why the extension is necessary

The time limit only starts once all the necessary information for processing it is received. This includes the time needed to verify a person's identity and/or to clarify their request.

Refusing a request

Where requests are manifestly unfounded or excessive, as described above, rather than charge a fee, if we prefer we can refuse to respond.

Where we refuse to respond to a request, without undue delay and at the latest within one month we must:

- Explain to the individual why we will not respond to their request,
- Inform them of their right to complain to the Information Commissioner and to a judicial remedy.

Verifying the identity of the requestor

We must verify the identity of the person making the request, using 'reasonable means'. This is because we must avoid personal data about one individual being sent to another, either accidentally or as a result of deception.

Format in which the data is to be provided

We will provide the information requested in permanent form. This will usually be either a print out, photocopy or USB. If the request is made electronically, we should provide the information in a commonly used electronic format, if the customer is happy with this.

Where we have used codes within data, we will explain these to the requestor so that the documents will make sense.

Third party data

This right to obtain information should not adversely affect the rights and freedoms of others. To make sure this does not happen, where records contain information relating to more than one person, we will consider whether it is reasonable in all the circumstances to disclose the information about the third party.

Our obligation is to provide information rather than documents; we may therefore delete names or edit documents if the third-party information does not form part of the requested information. This is known as “redacting information”.

Requests for large amounts of personal data

Where we process a large quantity of information about an individual, the legislation permits us to ask the individual to specify the information the request relates to.

There is no exemption for requests that relate to large amounts of data, but such requests could be considered manifestly unfounded or excessive (as explained above).

Exemptions and restrictions

In some circumstances we might have a legitimate reason for not complying with a subject access request, so legislation provides a number of exemptions from the duty to do so.

This might mean that we refuse to provide all or some of the information requested.

Enforced Subject Access Requests

It is a criminal offence, in certain circumstances and in relation to certain information, to require an individual to make a subject access request. If we suspect a subject access request is being made in these circumstances we will not comply with the request until we are satisfied the requester freely wants us to do so.

Right Three - The right to rectification

We have an obligation under data protection legislation to ensure that the information we hold about people is accurate and complete. If an individual believes that the information, we have is inaccurate or incomplete, they have the right to ask to have the record put right.

On receipt of a request, we must decide whether or not we agree that the data we hold is inaccurate or incomplete.

There may be occasions when data may have been correct at the time it was recorded, but later found to be inaccurate, for example a medical diagnosis which is later superseded by a different diagnosis. It will not always be appropriate in instances such as these to delete data, it might be more appropriate to ensure that the record is clear about what has happened.

Similarly, a record of an opinion may be an accurate record of that opinion, even if that opinion is wrong.

Requests for rectification will be considered in line with guidance on the subject from the Information Commissioner.

While we are looking at a request

While we are considering a request, we may need to restrict the use of the contested data (see the right to restrict processing below).

Timescale for response

A response must be provided to the requestor within:

- one month of receipt for standard requests
- three months of receipt where the request for rectification is complex

If data is decided to be inaccurate, the incorrect data may be struck through, rather than erased or blanked out. A clear note will explain the reason for the amendment; the note should contain details of who made the change and the Clerk who agreed the change.

If we have decided to take rectification action, if we have disclosed the personal data in question to third parties, we must inform them of the rectification where possible. We must also inform the requestor of any third parties to whom the data has been disclosed.

Where we are not taking action in response to the request, we must explain why to the individual and inform them of their right to complain to the Information Commissioner and to a judicial remedy.

Right Four - The right to erasure (the right to be forgotten)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for us to have it or use it. Detailed information about this right can be found on the ICO's website.

Deciding whether the right applies

There are some specific circumstances where the right to erasure **does not apply** and we can refuse to deal with a request.

While we are considering a request, we may need to restrict the use of the data in question (see the right to restrict processing below).

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

Much of the work of the Council will relate to the second and third categories above and consequently it will be exceptional for the right to erasure to apply to our data. However, each request for erasure will be considered on its merits and in line with Information Commissioner guidance.

Where the right to erasure **is determined to apply**, it does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the legislation).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Applications relating to children's data

There are extra requirements when the request for erasure relates to the personal data of a child.

Special attention must be given to situations where a child has given consent to processing and they later request erasure of the data, especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent. Guidance from the Information Commissioner will be followed in relation to any such requests.

Telling other organisations about the erasure of personal data

If it is decided to erase data and we have disclosed the personal data in question to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

If we have made the personal data public, we should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, where we process personal information online, for example on social networks, forums or websites, we must endeavour to comply with these requirements, unless there is a relevant exemption.

Timescale for action

Legislation requires that erasure be carried out 'without undue delay'.

Right Five - The right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data.

When processing is restricted, we are permitted to store the personal data, but not further process it.

We can retain just enough information about the individual to ensure that the restriction is respected.

We are required to restrict the processing of personal data in the following circumstances:

- Where we are considering a request for data rectification or for erasure (see above) or an objection to processing (see below).
- When processing is unlawful and the individual opposes erasure and requests restriction instead (they don't want their data to be completely erased)
- Where we no longer need the personal data but the individual requires the it to establish, exercise or defend a legal claim

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

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

Right Six - The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

When does the right to data portability apply?

The right to data portability only applies:

- to personal data the individual has provided to the Council;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means (electronic, not paper records)

The conditions are cumulative, and all must be met for a request to be successful.

As explained above, much of the data processing of the Council will be based on the need to fulfil our public tasks. As the right to data portability only applies to information processed based on consent and contractual obligations, it is unlikely to apply to much of our work.

Each request for portable data will be considered on its individual merits.

Responding to a request

When a request meets the criteria for data portability, we must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files.

Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation (if this is technically feasible). However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

Timescale

We must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or we receive a number of requests. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where we are not taking action in response to a request, we must without undue delay and at the latest within one month:

- Explain to the individual why we are not taking action,
- Inform them of their right to complain to the Information Commissioner and to a judicial remedy

Right Seven - The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Personal data processed for the performance of a legal task or our legitimate interests

Individuals are required to base their objection on "grounds relating to his or her particular situation".

We must stop processing the personal data 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

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. The right must be explicitly brought to the attention of the data subject and be presented clearly and separately from any other information.

Personal data processed for research purposes

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

Processing carried out online?

If any of the above activities are carried out online, we must offer a way for individuals to object online.

Personal data processed for direct marketing

What is Direct Marketing?

The factors that are used to identify direct marketing material are:

Directed to particular individuals - Lots of people receive “junk mail” that is not addressed to a particular person but to “the occupier”. This type of marketing is not directed at an individual and so is not direct marketing for the purposes of the Act. This kind of mail, posted through every letterbox on a street, includes leaflets like takeaway menus and information about clothing collections.

Communication by whatever means - The common image of direct marketing is that of mailshots or telemarketing. However, for the purposes of the Act it also includes all other means by which you might contact individuals, such as emails and text messages.

Advertising or marketing material - Direct marketing does not just refer to selling products or services to individuals. It includes promoting particular views or campaigns, such as those of a political party or charity. So, even if you are using personal data to elicit support for a good cause rather than to sell goods, you are still carrying out direct marketing.

Requests to stop Direct Marketing

If the request is in relation to direct marketing, for example a customer being sent a regular newsletter, we must stop the direct marketing as soon as we receive an objection. There are no exemptions or grounds to refuse.

We must:

- deal with an objection to processing for direct marketing at any time and free of charge
- inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be explicitly brought to the attention of the data subject and be presented clearly and separately from any other information.

You are not required to respond to a notice to stop direct marketing – it only requires you to stop. This is because you have no discretion about whether to comply with such a notice. However, acknowledging that you have received and acted on a notice is good practice, where this is appropriate

Timescale

Direct marketing must stop immediately an objection is received. The ICO recognises that a particular marketing campaign might already be underway when we receive a notice, and that the individual may subsequently receive further marketing material.

However, the ICO expects that in normal circumstances electronic communications should stop within 28 days of receiving the notice, and postal communications should stop within two months.

The service area undertaking the marketing should retain enough information to ensure that they are able to respect the request in future.

Right Eight - Rights in relation to automated decision making and profiling

Automated individual decision-making is a decision made by automated means with no human involvement in the decision-making process. Where this type of decision making takes place, individuals have the right to request that important decisions taken by us based on their personal information have some sort of human input.

Examples of this type of decision making might include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria

Profiling

Automated decision making may involve profiling. Profiling is the automated processing of personal data to evaluate aspects relating to a person, in particular to analyse or predict:

- performance at work,
- economic situation,
- health,
- personal preferences,
- interests,
- reliability,
- behaviour,
- location or movements.

Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals.

Based on the traits of others who appear similar, organisations use profiling to:

- find something out about individuals' preferences;
- predict their behaviour; and/or
- make decisions about them.

Automated individual decision making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The data protection legislation is designed to address these risks.

Restrictions on Automated decision-making about individuals, including profiling

Data protection legislation restricts us from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

Consequently, we can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by EU or UK law; or
- based on the individual's explicit consent.

If we are using special category personal data we can only carry out this type of processing if:

- we have the individual's explicit consent; or
- the processing is necessary for reasons of substantial public interest.

Special category data about a child is not permitted to be processed in this way.

We must identify any of our processing which falls into this definition and, for any that does:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that our systems are working as intended

At present the Council does not process any information by automated means without any human involvement.

This type of processing is considered high risk and should a service area consider processing data in this way, a Data Protection Impact Assessment will be essential, prior to the start of any such data usage.

Where there are no legal or similarly significant effects

If you are carrying out solely automated individual decision-making, but there are no legal or similarly significant effects, you can do so without additional restriction. You must however still comply with other data protection principles, in particular you must record your lawful basis for processing and advise individuals concerned of their rights.

Individuals have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

Legal consequences of a failure to comply with individual rights of data subjects

Referral to the Information Commissioner

Anyone who believes they are directly affected by the processing of personal data may ask the Information Commissioner's Office (ICO) to assess whether it is likely or unlikely that such processing complies with the legislation.

If the ICO's assessment shows that it is likely that the Council has failed to comply, they may ask us to take steps to comply with the data protection principles. Where appropriate, the ICO may order us to do so. The ICO has no power to award compensation to individuals – only the courts can do this.

The Information Commissioner may serve an enforcement notice if she is satisfied that we have failed to comply with the individual rights of data subjects. An enforcement notice may require us to take specified steps to comply with its obligations in this regard. Failure to comply with an enforcement notice is a criminal offence.

The Information Commissioner has a statutory power to impose a financial penalty on an organisation if she is satisfied that the organisation has committed a serious breach of the DPA that is likely to cause substantial damage or distress.

Enforcement by court order

If we fail to comply with the individual rights of data subjects, the requester may apply for a court order requiring us to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

If an individual suffers damage because we have breached data protection legislation, they are entitled to claim compensation from us. This right can only be enforced through the courts.