West Buckland Parish Council

DRAFT

Data Protection Policy

Adopted by the Council on 29th May 2018

Review date: May 2020

Contents

1. Aims

The Council aims to ensure that all personal data collected about staff, councillors, members of the public, contractors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs

	• Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Council processes personal data relating to staff, councillors, suppliers and others, and therefore is a data controller.
The Council is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our council, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the council of any changes to their personal data, such as a change of address
- Seeking professional advice in the following circumstances:
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - Deal with the transfer personal data outside the European Economic Area
    - If there has been a data breach
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our council must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff

– for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our staff and councillors.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the council holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Clerk. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

9.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of another individual

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time (where we have asked for consent to be given.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the clerk.

10. Photographs and videos

As part of our council activities, we may take photographs and record images of individuals.

We will obtain written consent from individual for photographs and videos taken for communication, marketing and promotional materials.

Uses may include:

- Newsletters, etc.
- Outside of the council by external agencies such as newspapers
- Online on our website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will where practical, delete the photograph or video and not distribute it further.

11. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).

- Completing privacy impact assessments where the council's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. Where necessary the appropriate advice will be sought.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters,
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our council and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on desks, in meeting rooms or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access laptops and other electronic devices.
- Passwords must be kept confidential and changed immediately if there is a suspicion that they have been compromised.
- No personal data is to be stored on removable media such as USB memory devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. Retention and Disposal of records

Records Management is the process by which the council manages all aspects of any type of 'record' whether internally or externally generated and in any format or media type, from their creation, throughout their lifecycle and to their eventual disposal.

13.1. Relevant Data Protection Principles

The data protection principles which directly relate to the management, retention and disposal of Personal Data are that the Personal Data must :

I. be accurate and kept up to date (Principle 4)
II. not be kept longer than necessary for the purpose for which it was obtained (Principle 5)
III. be processed by a Data Controller who has in place appropriate technical and organisational measures to prevent unauthorised processing and accidental loss, destruction or damage (Principle 7).

13.2 Retention Periods

In line with the fifth principle as set out at 16.1 (ii) above the Council will not retain Data any longer than necessary and in determining an appropriate retention period will take into account the following:

I. The current and future value of the Data.
II. The costs, risks and liabilities associated with retaining the Data.
III. The ease or difficulty in ensuring the Data remains accurate and up-to-date.

The standard default period for retaining Data will be based on the NALC Legal Topic Note 40: Local Councils Documents and Records.

13.3 Exceptions to the Retention Period

In the majority of cases Data will be securely disposed of when it reaches the end of the retention period. When assessing whether Data should be retained beyond the retention period the council will consider whether:

- The Data is subject to a request pursuant to the DPA.
- The council is the subject of, or involved in ongoing legal action to which the Data is or may be relevant.
  There is a greater public interest in retaining the Data.
- There are changes to the regulatory or statutory framework.

13.4 Disposal of Data

The destruction of Data is an irreversible act and must be clearly documented. All Data identified for disposal will be destroyed under confidential conditions.

The council may sub-contract to another organisation its obligations to dispose of Data under confidential conditions. Where the obligation to securely dispose of Data is sub-contracted, the council will satisfy itself of the subcontractor/third party's experience and competence to do so.

13.5 Manual Records

Where Data is held in paper or other manual form, the retention period has expired and none of the exceptions for retaining Data beyond the retention period as set out at paragraph 16.3 is satisfied, the council will ensure the Data is shredded or otherwise confidentially disposed of.

13.6 Electronic Records

Where Data is held in an electronic format the council will where feasible use its reasonable endeavours to:

I. Surround the Data with such technical and security measures to ensure it is not accessible other than by a Data Processor.

When the data is no longer required:

II. Permanently delete the Data from the council electronic systems when and where this becomes possible.

Where the steps set out at paragraph 13.6 II are complied with, the council considers the Data to be 'put beyond use' and this Data will not be used in order to respond to a Subject Access Request.

14. Personal data breaches

The council will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours.

15. Training

All staff and councillors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the council's processes make it necessary.

16. Monitoring arrangements

The council is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our council's practice. Otherwise, or from then on, this policy will be reviewed annually by the council.

17. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- General Privacy Notice
- Privacy notice for Staff, Councillors and Other Roles.

Appendix 1

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- The clerk will investigate the report, and determine whether a breach has occurred. To decide, the clerk will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The clerk will alert the chair
- The clerk will make all reasonable efforts to contain and minimise the impact of the breach, assisted by any data processors where necessary.

- The clerk will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The clerk will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the clerk will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the clerk must notify the ICO.
- The clerk will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within our network storage system.
- Where the ICO must be notified, the clerk will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the clerk will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the clerk
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the clerk will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the clerk expects to have further information. The clerk will submit the remaining information as soon as possible
- The clerk will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the clerk
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The clerk will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The clerk will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- A records of all breaches will be retained.
- The clerk and council will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible