Bledlow-cum-Saunderton Parish Council Data Protection Policy

Date Adopted: 6th August 2020

Date to be Reviewed: May 2021

1 INTRODUCTION

1.1 This Data Protection Policy (**"Policy"**) sets out the responsibilities and procedures for using personal data within Bledlow-cum-Saunderton Parish Council (**the Council** or **we** and **us**).

1.2 This Policy applies whenever we collect or handle personal data in any way.

1.3 Everyone has rights over the handling of their personal data. In performing its functions, the Council will collect, store and use personal data about members of the Council, its staff and members of the public.

1.4 A breach of this Policy may result in legal consequences and, where appropriate, disciplinary action being taken.

2 AIMS OF THE POLICY

2.1 To set out the rules on collecting, handling, using, transferring and storing personal data.

2.2 To protect the rights and freedoms of individuals when the Council uses personal data.

2.3 To help the Council, our members and our staff to understand the fundamentals of data protection laws and to comply with those laws.

2.4 To explain the risks to the Council if we do not comply.

3 WHAT DOES THE LAW SAY?

What is the GDPR?

3.1 The General Data Protection Regulation ("**GDPR**") is an EU Regulation which, together with the UK Data Protection Act, aims to give individuals extensive rights over the handling of their data. In this Policy we use "data protection laws" to refer to these laws and regulations.

What is personal data?

3.2 Personal data is any data that relates to a living individual who is identifiable from that data (or from that data and other information). It therefore captures a wide range of data, including names, contact information, date of birth, photographs and even an IP address. If you are unsure about whether certain information is personal data, please speak with our Clerk (see paragraph 4 of this Policy for contact details).

What are special categories of personal data?

3.3 Data protection laws class a certain type of personal data as particularly sensitive. This will include information about political opinions, racial or ethnic origins, health data, sexual orientation and biometrics It is important that you recognise these special categories, because the law imposes more stringent requirements on their use and may mean you:

- need the consent of the individual whose personal data you are using; or
- need to rely on another exemption before you are lawfully able to process the data.

Who regulates the GDPR in the UK?

3.4 In the UK, the Information Commissioner's Officer (**ICO**) independently enforces data protection laws.

What happens if we get it wrong?

3.5 The ICO has a wide range of powers including:

- levying significant fines;
- issuing enforcement notices requiring data breaches to be remedied; and

- publicising breaches on the ICO's website.

The ICO has made it clear that it will take data breaches very seriously, even if a breach results from our data being unlawfully accessed/hacked. If we are to avoid significant fines and reputational damage, it is essential we take the greatest care when handling personal data.

The data protection principles

3.6 Data Protection Laws are based on the following principles/requirements:

(1) **Fair, lawful and transparent.** Personal data must be processed fairly, lawfully and transparently. While data protection laws do not intend to prevent us processing personal data altogether, they are there to ensure that we do it fairly and without adversely affecting the rights of the individuals whose data we are using. The privacy notices we send to customers, staff and others form part of this drive for transparency.

(2) **Use for limited purposes.** We must collect personal data for specified, explicit and legitimate purposes and we must not process it in a manner incompatible with those purposes. While at the Council , we may be collecting personal data in different ways, we must only use it for the purpose(s) for which we receive it and must not use the data for any other purpose.

(3) **Data minimisation.** Personal data must be adequate, relevant and limited to what is necessary. We should only collect, use, access or analyse personal data to the extent that we need to. We should ask ourselves: are we doing the minimum amount necessary with personal data to achieve our purpose?

(4) **Accuracy.** Personal data must be accurate and, if necessary, kept up to date. We should check the accuracy of any personal data when collecting it, and at regular intervals afterwards. We should take all reasonable steps to destroy or amend inaccurate or out-of-date data.

(5) **Data retention.** We must keep personal data for no longer than necessary. This will vary depending on the data in question. Organisations like the Council may keep a separate Data Retention Policy to guide us in deciding how long to keep information and when we should delete or destroy it. Please refer to any such policy for further details to make sure we comply with it.

(6) **Respecting an individual's legal rights.** We must process personal data in accordance with the rights of data subjects (i.e. the individuals whose personal data we are is using). See paragraphs 8 and 9 below for further details about rights of access (commonly known as a "subject access request" or **SAR**) and the right for information to be deleted (often referred to as the right to be forgotten).

(7) **Integrity and confidentiality**. We must process personal data in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use and accidental loss, destruction or damage. This principle is critically important as, historically, data losses due to poor security have resulted in the biggest fines. The GDPR says that we must use "appropriate technical and organisational measures".

(8) **International transfers.** Personal data must not leave the UK and the European Economic Area unless certain legal protections are in place. If we become aware of personal data leaving the UK (for example, we might be using an application provided by a company with servers storing personal data in, say, Japan or the United States), we must inform the Clerk immediately.

Accountability

3.7 The GDPR also introduces the principle of accountability. Broadly, this means that we must be able to demonstrate the steps the Council is taking at all levels of the organisation to ensure that we follow the data protection principles above. This Policy forms part of that effort, but ultimately the best way of showing accountability is if we all take personal ownership and responsibility for complying with these data protection laws.

Controller or processor?

3.8 Our obligations under data protection laws will vary depending on whether we are acting as a data controller or data processor. We act as **data controller** when we decide the purposes for which we process the data, and how we do it. We act as **data processor** when we hold data on someone else's behalf and follow their instructions.

3.9 However, for this Policy, we apply the same standards of care to **all** personal data that we hold, whether we act as data controller or data processor. This is good business practice and will help us to comply with our obligations on data handling.

4 WHO CAN I SPEAK WITH ABOUT DATA PROTECTION ISSUES AT THE COUNCIL?

If you have any questions about this Policy, or any concerns that we have not followed the Policy, , please email the Clerk at clerk@bcspc.org.uk.

5 TAKING OWNERSHIP

The GDPR introduces a new requirement called data protection by "**design and default"**. It essentially means that we all have a responsibility to proactively build the principles in paragraph 3.6 above into our everyday activities. Don't be afraid to question current or old practices or technology if you think they do not follow good data protection practice and don't forget to inform the Clerk if you are looking at new ways of collecting or storing data.

6 DATA BREACHES

6.1 A personal data security breach is any security breach leading to the accidental or unlawful destruction, loss, alteration, disclosure of, or access to, personal data. It could be as a result of a cyber-crime. Or it could be that we have shared personal data with another organisation or person without permission. It may be accidentally sending an email attachment to the wrong person, leaving confidential information about a person or group of people on public transport (or some other public place) or losing a laptop, device or notes.

6.2 Whatever the issue is, **tell the Clerk about it immediately**. The Clerk will in turn follow the breach notification procedure, which contains a list of additional questions on which we will need help. This will include gathering information on how the data breach happened, who has been affected and other relevant background details.

6.3 We need to do all of this because the GDPR requires the Council to report certain personal data breaches to the ICO, and to the individuals affected, within 72 hours of first becoming aware of it. For that reason, we need to act quickly. **However, do not report the breach to the ICO directly as the Clerk will arrange for this to be done.**

7 SHARING INFORMATION WITH OTHER ORGANISATIONS

7.1 If we:

- are looking at engaging a new partner/supplier; and

- know that the partner/supplier will be obtaining or using personal data relating to the general public or the Council 's staff or officers,

we will need to contact the Clerk as soon as possible before engaging with them.

7.2 The GDPR requires the Council to

- vet these partners/suppliers to ensure they offer an appropriate level of security;
- make sure that there is a written contract between the partner/supplier and the Council ; and
- ensure that this written contract is GDPR compliant.

7.3 If the intention is to hold personal data outside the EU, for example, we will need to take some additional steps before we can provide that data to the new partner/supplier. The key thing is to contact the Clerk before disclosing personal data so we can put in place the necessary protections.

8 DEALING WITH SUBJECT ACCESS REQUESTS (SAR)

8.1 An SAR is a request from an individual asking for a copy of the information the Council holds about them. This is a statutory right which we have to comply with, in most case, within one calendar month after receiving the request. If we receive a SAR, or something we think may be a SAR, we should **immediately** notify the Clerk who will then provide all necessary assistance. **Please do not respond to the individual without first consulting with the Clerk**.

8.2 A SAR does not need to be in writing to be valid, nor does it require any other particular formalities. It does not need to be addressed to any particular person in the Council, and it can be verbal or by email, post, fax, text or possibly even social media. The individual issuing a SAR could be a member of the public, a councillor or a member of staff.

8.3 While individuals have broad rights to ask for information that the Council holds, these rights are not unlimited. The Clerk will be able seek guidance on the necessary steps and whether there is an exemption to making a particular disclosure. If the Council is processing personal data on behalf of someone else (the data controller), the first step is likely to involve notifying that person. It is the data controller who will have primary responsibility for responding to the SAR, and the Council will need to work with them to allow this to happen in good time.

9 "RIGHT TO BE FORGOTTEN" REQUESTS

9.1 A "right to be forgotten" request is a written request from an individual to have information that the Council holds about them erased, for example if it is inaccurate or no longer necessary. Like SARs, this is a statutory right but not an unconditional one. Please contact the Clerk **immediately** if you receive a request. **Do not respond to the individual directly.**

9.2 As indicated elsewhere in this Policy, the Council can only process personal data if it has lawful grounds for doing so. For example, to perform its statutory functions or comply with the law. Once those lawful grounds no longer exist, the Council should stop processing the data. The individual's right to be forgotten is therefore just another way for an individual to ensure that we comply with our obligations under data protection laws to only process data to the extent we need to and for no longer than necessary.

10 CHANGES TO THIS POLICY

The Council reserves the right to change this Policy at any time with or without notice. If the changes are significant, we will tell you about them.