**Biddulph Town Council**

**IMPLEMENTATION OF GENERAL DATA PROTECTION REGULATIONS**

# **WRITTEN BY:**

Mrs Sarah Haydon, Chief Officer

# **CREATED:**

April 2019

# **APPROVAL DATE:**

Town Council – 16 April 2019

# **REVIEW DATE:**

April 2021

# **INTRODUCTION**

1.1 The General Data Protection Regulation (GDPR) took effect in the UK from 25 May 2018.

Along with the Data Protection Act (DPA) 2018, it replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by councils.

Local councils and parish meetings must comply with its requirements, just like any other organisation.

1.2 The GDPRs main concepts and principles are very similar to those contained in the previous Data Protection Act 1998.

Biddulph Town Council complied with the Data Protection Act 1998 and applied two polices in relation to the publication and management of information and data:

* Publication Scheme and Guidance
* Information Management and Data Protection Policy

These policies are being reviewed to ensure compliance in relation to Freedom of Information and retention of documents. The Data Protection references will be removed.

1.3 One of the main changes is that the GDPR places a much greater emphasis on transparency, openness and the documents needed, in order to show that the Town Council are complying with the legislation. This is incorporated within the idea of ‘accountability’.

1.4 **Appendix A** is a summary of the main differences between the Data Protection Act 1998 and GDPR.

# **OBJECTIVES OF THIS DOCUMENT**

2.1 The GDPR has a number of underlying principles. These include that personal data:

* Must be processed ***lawfully, fairly and transparently***.
* Is only used for a ***specific processing purpose*** that the data subject has been made aware of and no other, without further consent.
* Should be ***adequate, relevant and limited*** i.e. only the minimum amount of data should be kept for specific processing.
* Must be ***accurate*** and where necessary ***kept up to date***.
* Should ***not be stored for longer than is necessary***, and that storage is safe and secure.
* Should be processed in a manner that ensures ***appropriate security and protection*.**

The aim of this document is to provide an overview of the legislation and to highlight that Biddulph Town Council satisfies the requirements through processes implemented and strengthened.

# **DETAILS OF THE LEGISLATION**

3.1 Generally, the rights of individuals that are granted under the GDPR are the same as under the DPA 1998, but with some significant additions.

The GDPR includes the following rights for individuals, which are briefly explained here:

**The right to be informed**

* Individuals continue to have a right to be given "fair processing information", usually through a privacy notice. Under the GDPR there is additional information that the Town Council will need to supply.
* For example, the Town Council will have to explain the lawful basis for the processing of their data; the data retention periods (how long the Town Council keep it for) and that individuals have a right to complain to the ICO if they think that there is a problem in the way that the Town Council deal with their personal data.

**The right to access (includes subject access requests)**

* Under the GDPR the right of data subjects to request information about the personal data processed by councils remains largely the same. However, under the new regime councils must respond without undue delay and in any case within one month of receipt of the request.
* Additionally, the £10 fee for making a request has been abolished which is likely to lead to a greater number of requests. It is estimated that 25% of requesters previously withdrew or did not pursue their request when asked to fill in a form and pay the £10 fee. Councils will need to consider if they have sufficient resources to deal with an increase in the volume of data subject access requests.
* The Town Council can refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If the Town Council do refuse a request the Town Council must tell the individual why and that he/she has the right to complain to the ICO or go to court. The Town Council should also keep a record of the reasons and decision process.

**The right to rectification (correction)**

* Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, the Town Council must tell those third parties of the correction. The Town Council must also tell the individuals about the third parties to whom the data has been given.

**The right to erasure (also known as the right to be forgotten)**

* Data subjects have the right to request the removal or erasure of their personal data, for example if it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent. Not only will councils need to comply with such requests, but they will also need to ensure that any third party with whom the data was shared also deletes such data.
* This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent. This is one reason why consent is not the best lawful basis for data processed in connection with a person’s role in the council.

**The right to restrict processing**

* Individuals have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes his/her personal data is inaccurate or he/she objects to the processing). If processing is restricted, the Town Council can still store the data but cannot otherwise use the data.

**The right to data portability**

* Data subjects have the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. Councils should consider how and where the personal data is held and if such data can be easily transferred in a safe, secure manner without impacting the usability of such data by the data subject. The council will need to comply with such requests without undue delay, and in any event within one month.
* This is a new right introduced by the GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT system to another.

**The right to object**

* Individuals have the right to object to processing in certain circumstances - e.g. if a council has relied on one lawful ground to process data without consent and an individual is not happy with this they have the right to object to the council processing their data.
* The right not to be subject to automated decision-making including profiling
* The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. This right is similar to that contained in the DPA 1998.

3.2 The GDPR sets out ***six lawful bases*** for processing data.

Unless an exemption applies, ***at least one of these will apply in all cases***. It is possible for more than one to apply at the same time. For example, a council may be processing personal data about a staff member in connection with an employment contract and at the same time have a legal obligation to process the same personal data.

The six lawful bases for processing personal data under the GDPR are:

* **Consent**

A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language.

Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject’s wishes – either by a statement or by a clear affirmative action.

* **Legitimate interests**

This involves a balancing test between the controller (or a third party’s) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

* **Contractual necessity**

Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

* **Compliance with legal obligation**

Personal data may be processed if the controller is legally required to perform such processing (e.g. complying with the requirements of legislation).

* **Vital Interests**

Personal data may be processed to protect the ‘vital interests’ of the data subject (e.g. in a life or death situation it is permissible to use a person’s medical or emergency contact information without their consent).

* **Public Interest**

Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

# **HOW DOES THE TOWN COUNCIL ENSURE COMPLIANCE?**

4.1 Biddulph Town Council registers annually with the Information Commissioner’s Office (ICO) as a Data Controller. In addition, the Town Council pays the registration fee for Town Councillors (only) to ensure their activities are covered.

4.2 Staff have been trained in the requirements of GDPR to ensure activities are compliant.

4.3 This policy establishes the principles within which the Town Council operates.

4.4 In ensuring that the Town Council is compliant, a number of back-office activities have been undertaken:

* An internal register of processing activities has been completed;
* A lockable cabinet has been purchased; this is kept locked at all times to ensure that personal data is not left on desks;
* A consent form has been implemented;
* All staff use password-protected computers with unique (regularly changed) passwords; passwords are not written down;
* A personal data audit has been undertaken; and,
* A Privacy Notice has been added to the Town Council website.

Actions identified as part of the above activities have been implemented.

# **SUBJECT ACCESS POLICY AND RESPONSES**

5.1 A **subject access request** (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for.

5.2 **What will Biddulph Town Council do upon receipt of a SAR**

* Verify whether the Town Council is the controller of the data subject’s personal data. If the Town Council is not a controller, but merely a processor, inform the data subject and refer them to the actual controller.
* Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
* Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.
* Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, the Town Council may refuse to act on the request or charge a reasonable fee.
* Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
* Verify whether the Town Council processes the data requested. If the Town Council does not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.
* Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
* Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

5.3 **Responding to a SAR**

Respond to a SAR within one month after receipt of the request:

* If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;
* If the council cannot provide the information requested, it should, inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
* If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.
* If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:
* the purposes of the processing;
* the categories of personal data concerned;
* the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses;
* where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
* the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
* the right to lodge a complaint with the Information Commissioners Office (“ICO”);
* if the data has not been collected from the data subject: the source of such data;
* the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
* Provide a copy of the personal data undergoing processing.

# **SECURITY INCIDENT RESPONSE**

6.1 A data breach of any size is a crisis management situation, which could put an entire council at risk. Data security is not an IT issue, it is an organisational risk, and breach response should involve people from a number of roles across the council.

Planning for a breach is therefore essential; every council should have in place a breach response plan, and should designate, in advance, a breach response team which can be convened at short notice to deal with the crisis.

Understanding the issues that arise in a breach situation, and practising managing a breach, are essential to effective breach response. Failure to plan and practise increases the regulatory, litigation and reputation risk to the entire council.

Whilst the Town Council note that the likelihood of a security incident is low, appropriate measures are in place to ensure that the risks are further reduced. This is reviewed regularly.

# **CYBERSECURITY**

7.1 Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

Many of the steps that councils can take to limit the risk and impact of a personal data breach are relatively simple to implement, but require effective policies and controls to implement. Good information security crosses over a number of policies.

At present, IT services are provided by Staffordshire County Council. This will be reviewed regularly.

**Appendix A**

| ***Change*** | ***Detail of Change*** | ***Impact of Change*** |
| --- | --- | --- |
| **Record Keeping** | Each Data Controller must maintain a record of processing activities under its responsibility. Data Processors must also keep a record of the processing activities they carry out on behalf of a Data Controller. | The level of detail is the same as contained in an ICO registration / notification at present and the log can be requested at any time by the ICO.  |
| **Privacy Notices** | Under the GDPR, privacy notices must contain more information, be more transparent, use clear and plain language, and must be easily accessible.  | Privacy notices will need to be reviewed and updated to make them clearer, more transparent and easily accessible.  |
| **Consent** | The way consent is obtained will change under the GDPR as individuals have more rights to decide how their data is processed. Where processing personal data is based on consent, the council must be able to evidence the consent. Consent must be by an “opt in” method. | The types of processing activities which require the consent of an individual need to be identified and consents must be captured in a GDPR compliant manner.  |
| **Breaches** | Data Controllers must report personal certain types of data breaches to the ICO without ‘undue delay’, and where possible no later than 72 hours after having become aware of the breach. An individual who has suffered damage as a result of a breach can claim compensation from the Data Controller or the Data Processor.  | How councils handle data breaches should be reviewed. Training will be required to increase awareness of what constitutes a breach and how to escalate investigations into breaches.  |
| **Right of Access (Subject Access Requests)** | The time limit to comply with a Subject Access Request (“SAR”) has been reduced from 40 calendar days to one calendar month. The ability to charge £10 per SAR has been removed so all SARs are free of charge from 25th May 2018. | The SAR process will need to be reviewed and updated accordingly.  |
| **Data Privacy Impact Assessments (“DPIA”)** | The GDPR makes it mandatory for DPIAs to be carried out in certain situations. DPIAs will need to contain a description of the processing and the purpose of the processing and need to identify any risks to the personal data and the rights and freedoms of individuals, and the measures and safeguards implemented to mitigate these risks.  | DPIAs will need to be introduced where new technologies are used (e.g. CCTV or other monitoring) for high risk data processing activities (e.g. large-scale processing of sensitive personal data) or when there are systematic and extensive activities which use automated processing to evaluate, analyse or predict behaviour (e.g. tracking behaviour on a website).  |
| **Privacy by Design** | When developing, designing or using services or applications which involve processing personal data, Data Controllers and Processors should adopt internal policies and measures to ensure personal data is protected. | If councils introduce new IT systems or launch new websites which collect personal data, these new systems should have data protection controls built into their designs from the outset.  |
| **Right to Object to processing** | Individuals must be advised of their right to opt out of processing activities, including marketing.  | “Unsubscribe” methods will need to be reviewed. Any reasonable requests to object to processing should be stored and evidenced.  |
| **Right to Erasure** | An individual has a right to request that their personal data is deleted. A Data Controller must delete personal data unless there is a legal obligation to retain the personal data. | Data deletion processes will need to be introduced so that data is not retained indefinitely. It’s likely a “data cleansing” exercise will need to be carried out prior to 25th May 2018 so that the council is not storing data it no longer requires or has a need to retain. |
| **Profiling** | An individual has the right not to be subject to a decision based solely on “automated processing”, including profiling. This is where a computer, or computer software rather than a human makes a decision about an individual. | Activities that rely or use automated decision making need to be identified. Processes need to be put in place to allow, where possible, individuals to object to automated decision making (and e.g. request that a human intervenes to make the decision).  |
| **Data Protection Officer** | A Data Protection Officer (DPO) may need to be appointed by councils if the Town Council process personal data for regular monitoring of individuals, or any sensitive personal data, on a large scale. The DPO should report to the highest level of management (i.e. full council) and must be informed about all data protection issues within the council. | Clerks and RFOs cannot be designated as a council’s DPO because they are unlikely to satisfy all of the requirements of the job.  |
| **Right of Portability** | The GDPR introduces a new right of data portability. This right allows for the data which an individual provided to the Data Controller to be provided to the individual in a structured format, to allow it to be provided to another Data Controller. | It will be important to understand where the data is being stored and in what format to make it easier to move personal data (and receive personal data from other data controllers). |