



GENERAL DATA PROTECTION REGULATIONS, CONFIDENTIALITY AND INFORMATION MANAGEMENT POLICY

WRITTEN BY:

Esther Gladstone, Finance and Administration Officer

REVIEWED:

July 2021

APPROVAL DATE:

Finance Strategy and Management Committee – 27 July 2021

Town Council – 14 September 2021

REVIEW DATE:

September 2022

INTRODUCTION

- 1.1 This policy replaces the 'Implementation of General Data Protection Regulations' and the 'Information Management and Data Protection Policy' previously adopted by Biddulph Town Council.
- 1.2 In the course of carrying out its duties and powers, Biddulph Town Council holds and retains personal data, some of which is considered sensitive personal data. This policy outlines how personal data and confidential information will be managed to ensure that the Town Council is compliant with legislation and maintains high standards in relation to its data management.

SUMMARY OF POLICY

- 2.1 The Town Council is a data controller and therefore has obligations related to the personal data held when carrying out its functions. The Council is responsible for any council business conducted involving personal data on any device or through any email account.
- 2.2 Councils must ensure the confidentiality, integrity and availability of all personal data they hold, even if the data is being processed through personal email accounts or is stored on a privately owned device. Therefore, all Officers and Councillors receiving information on behalf of the Council must ensure that all information is obtained and processed in accordance with the key principles and objectives of the General Data Protection Legislation.
- 2.3 A number of processes are in place to ensure information security within the Town Hall, and Town Council IT systems.
- 2.4 The use of the privately owned devices or personal email address for any information involving personal data is problematic. Therefore the amount of personal data on such devices or accounts should be minimised and measures taken to manage the risk that is presented where such use is unavoidable.

LEGISLATION

- 3.1 The main body of legislation covered in this policy relates to the UK-GDPR and the Data Protection Act 2018.
- 3.2 Though the General Data Protection Regulation (GDPR) are a European Law, it was enshrined in UK law under the Data Protection Act 2018. Following the end of the 'Brexit' transition period on 31 December 2020, the European GDPR were incorporated directly in to UK law with minor technical amendments. This is now known as UK-GDPR.
- 3.3 EU GDPR legislation still applies to any users of Biddulph Town Council's services or products within the EU. The only instance where this is likely to apply is for European users of the Website and any personal information relating to Biddulph's Twinned Town of Fusignano.

SUMMARY OF UK-GDPR LEGISLATION

4.1 In order to comply with the UK-GDPR and Data Protection Act 2018, Biddulph Town Council must ensure that the following principles are adhered to in terms of personal data.

- It must be processed **lawfully, fairly and transparently**.
- It is only used for a **specific processing purpose** that the data subject has been made aware of and no other, without further consent.
- It should be **adequate, relevant and limited** i.e. only the minimum amount of data should be kept for specific processing.
- It must be **accurate** and where necessary **kept up to date**.
- It should **not be stored for longer than is necessary**, and that storage is safe and secure.
- It should be processed in a manner that ensures **appropriate security and protection**.
- The controller shall be responsible for, and be able to demonstrate compliance with the above points (accountability)

4.2 The legislation also sets out the following rights of the individual about whom data is held:

- The right to be informed.
- The right to access (includes subject access requests).
- The right to rectification.
- The right to erasure (also known as the right to be forgotten).
- The right to restrict processing.
- The right to data portability.
- The right to object.

4.3 There are six lawful bases on which data can be processed, upon which at least one must apply in all instances where data is processed, unless an exemption applies:

- Consent – informed consent must have been clearly given and should be able to be withdrawn.
- Legitimate interests.
- Contractual necessity – it is necessary to process personal data in order to enter in to a contract with a person, for instance, allotment tenancies.

- Compliance with legal obligations.
- Vital Interests.
- Public Interest.

4.4 It is not possible to list all the possible reasons for exemption within the scope of this policy, nor should exemptions be relied upon except for specific individual cases, however, where they are required, the data protection legislation shall be referred to.

GENERAL UK-GDPR COMPLIANCE MEASURES

- 5.1 As per Section 7(3) of the Data Protection Act 2018, Parish Councils are not considered to constitute a Public Authority for the purposes of UK GDPR. As a result, Biddulph Town Council is not required to appoint a Data Protection Officer. However, the Town Council is required to ensure that there are sufficient staff and resources to discharge its obligations under the UK GDPR.
- 5.2 When an Officer or Councillor receives or records any personal information on behalf of Biddulph Town Council, they must be clear for what purposes, and under what GDPR principles, the information is being obtained and processed. This information must be maintained securely for no longer than is necessary and shared only with those who have a legitimate reason to be provided this information.
- 5.3 To assist with ensuring GDPR compliance, an annual audit of all data collection and processing activity is undertaken. Each activity is assessed to ensure that it adheres to the overarching aims, principles and objectives of the UK-GDPR. This audit is also undertaken before implementing any new administrative systems.
- 5.4 To ensure that the public maintain their right to be informed, a General Privacy Notice is available on the Biddulph Town Council website and copies may be obtained from the Town Hall.
- 5.5 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.

- 5.6 Where an activity may result in high risk to personal freedoms, a Data Protection Impact Assessment will be undertaken. There are unlikely to be situations where Biddulph Town Council's activity falls into this category, but an instance where this may apply to a Town Council could be if undertaking an installation of CCTV for monitoring a public area. Any significantly new processes involving personal data or monitoring should be thoroughly checked against legislation.

MAINTAINING CONFIDENTIALITY AND SECURITY ON BIDDULPH TOWN COUNCIL IT

- 6.1 Biddulph Town Council maintains two WiFi networks at the Town Hall. To minimise the risk to any data transferred or stored using the Staff WiFi Network, this network is only usable by Officers of the Town Council, Councillors and tenants who have signed a Wifi Network Sharing agreement with the Town Council. For all other purposes, the guest network must be used. The Staff network password must not be given to anyone other than those outlined above.
- 6.2 Both the WiFi network and IT provision are managed by external companies to ensure adequate cybersecurity measures are in place. Should there be any questions or concerns regarding potential breaches or security, this should be raised with the holders of the relevant contract.
- 6.3 Users of Biddulph IT systems must ensure they have an appropriately secure password for their network login which can not be easily guessed or found by others.
- 6.4 Computers must be locked or turned off when not in use or left unattended.
- 6.5 Computer users must make sure their computer screen is not visible to anyone unauthorised to see the information, for instance – ensuring their computer is turned away from a window where the general public are able to look in.

- 6.6 Town Council owned phones must be password protected and set up for remote locking and wiping should the need arise.

MAINTAINING CONFIDENTIALITY AND SECURITY ON PAPER RECORDS

- 7.1 By the very nature of the Town Council's activity, a significant amount of paperwork which is either confidential or contains personal identifiable information is maintained.
- 7.2 Any personal information held by the Council is held in either a locked draw or locked room for which only authorised people are provided access.
- 7.3 Personal information is not removed from the office other than where completely necessary (for instance taking the interment paperwork when witnessing an burial or interment of cremated remains). Where such necessary activity is undertaken, it must be kept with the person at all times.
- 7.4 Should an event happen where a paper copy that contains confidential or personal information is lost or stolen, this must be reported immediately to the Chief Officer.
- 7.5 Agendas and publicly available Minutes must not contain personal information other than that which is already in the public domain. However, confidential items may well be included within Officer and Councillor copies of minutes and therefore must be treated with the same level of caution.
- 7.6 Paper copies of confidential or personal information that are no longer required must be shredded or suitably destroyed (i.e. ensuring there is no way of retrieving that information from the papers)

ISSUES RELATING TO PERSONAL EMAIL ACCOUNTS AND PRIVATELY OWNED IT DEVICES

ACCEPTABLE USE OF PERSONAL DEVICES AND EMAIL ACCOUNTS

- 9.1 Despite the problems associated with personal devices, at present some use is unavoidable. Therefore personal devices and email for Council business should only be used where there is no reasonable alternative option, and only when sufficient measures are in place to manage the risk.
- 9.2 All personal devices used for Council business must be pin and passcode secured and have a facility to remotely wipe data. They must only be used on WiFi networks with an appropriate level of security.
- 9.3 It should always be endeavoured to ensure that no personal information is sent to personal email addresses or downloaded on to personal devices. Anonymising or removing the personal information from an email or attachment may allow the information to be shared in a low risk way. The personal information, if needed and adheres to the principles outlined in the GDPR, may then be provided over the phone, thus preventing the physical storage or retention of such information.
- 9.4 Where the downloading or retaining of information on a personal device or the sending of personal information to a personal email account, is unavoidable, the following must be adhered to:
- Only the minimum and least identifiable method of sharing the information should be given (for instance using initials rather than a full name).
 - Documents must be appropriately encrypted and password protected. The password for the information must not be sent via email, but rather provided over the phone. A text message may be acceptable if the email is not accessible from that phone.
 - Any email that includes personal information must contain a statement that informs the user that personal information is contained within, and must be only used for the intended purposes and deleted immediately when the information is no longer required.
 - The receiver of the email must have previously agreed to receive this information and handle in accordance with the IT Acceptable Use Agreement (which includes deleting the information as soon as possible.)

- 9.5 Where a person becomes aware of a privacy breach on a network, device or email account that contains information relating to Council business, they must inform the Chief Officer immediately so appropriate remedial action and reporting can take place. This includes reporting where an email is hacked, phishing software located or where a device is lost or stolen.
- 9.6 To improve the standards of information security within Biddulph Town Council, by the end of 2021 all Councillors will be granted a Biddulph Town Council email address which should be used for all Biddulph Town Council related business. As per the IT acceptable use agreement, emails to Biddulph Town Council email addresses must not routinely be forwarded to any other personal or organisational email addresses held by the same Councillor, other than in exceptional circumstances and only where the measures in place under section 9.4 are adhered to. This means that it is not permissible to put an auto-forward on for emails to be automatically sent to a personal, business, District Council or County Council email address.

SUBJECT ACCESS POLICY AND RESPONSES

- 10.1 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.
- 10.2 **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.
 - Verify 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.

10.3 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

- 11.1 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.
- 11.2 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.
- 11.3 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.
- 11.4 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.

MAKING INFORMATION AVAILABLE

12.1 The Model Publication Scheme

This document is a means by which the Council can make a significant amount of information available routinely, without waiting for individuals to request it. The Scheme is intended to encourage people to take an interest in the work of the Council and its role within the

community. The aim is to make it easier for the public to access information. In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. Further information is available in the **Publication Scheme and Guidance** document.

12.2 **Meetings**

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the website and sent to the local media. Meeting agendas will be published on the website, and if requested emailed by the Chief Officer to members of the public. The Council publishes an annual programme in May each year. All formal committee meetings, are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council meeting agenda.

12.3 **Matters of confidentiality**

Occasionally, Council or Committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

12.4 **Local Government Transparency Code 2015**

The Code details information that must be published quarterly. Where Biddulph Town Council has expenditure exceeding £500, this information must be available to the public. This must include:

- Date the expenditure occurred.
- Local authority department that incurred the expenditure.
- Beneficiary.
- Summary of the purpose of the expenditure.
- Amount.
- VAT that cannot be recovered.

This information is routinely considered by the Town Council and published online.

12.5 Biddulph Town Council must also publish details of every invitation to tender for contracts to provide goods and/ or services with a value that exceeds £5,000. This must include:

- Reference number.
- Title.
- Description of the goods and/or service sought.
- Start, end and review dates, and
- Local authority department responsible.

Similar information must also be published in relation to contracts that are entered into by the Town Council, in excess of £5,000. This must include information about whether the contract was a result of an invitation to quote or a published invitation to tender. The size of the supplier must also be made available.

12.6 Of the information that must be published annually, Biddulph Town Council publishes online details of land and assets, grant allocations and details of the organisation chart.