Northleach with Eastington Town Council

DATA PROTECTION POLICY Adopted September 2019

1. Introduction

1.1. Northleach with Eastington Town Council takes its responsibilities with regards to the management of the requirements of the General Data Protection Regulation (GDPR) seriously.

1.2. The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 (the 1998 Act) in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Act 2018 (the DPA 2018). The GDPR sets out requirements for how organisations need to handle personal data.

1.3. The council obtains, uses, stores and otherwise processes personal data relating to councillors and staff, former councillors and staff, current and former contractors, website users and members of the public, collectively referred to in this policy as data subjects.

1.4. When processing personal data, the council is obliged to fulfil individuals' reasonable expectations of privacy by complying with General Data Protection Regulation (GDPR) and other relevant data protection legislation (Data Protection Act 2018).

1.5. This policy therefore seeks to ensure that the council is clear about how personal data must be processed and the council's expectations for all those who process personal data on its behalf.

2. Scope & Responsibilities

2.1. This policy applies to all personal data processing carried out by the council, regardless of the location where that personal data is stored (e.g. on an employee or councillor's own device) and regardless of the data subject.

2.2. Anyone processing personal data on the council's behalf must read and comply with this policy.

2.3. The council is responsible for ensuring compliance with this policy, and will implement appropriate processes, and provide information and training so that anyone processing personal data on the council's behalf knows what to do.

2.4. The council will work to identify areas that might cause compliance issues and use this to inform the council's risk assessments, and to improve its data processing processes and controls.

2.5. The GDPR sets a high standard for consent. It is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

2.6. When relying on consent you must keep clear records to demonstrate that you have gained compliant consent.

2.7. The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw their consent and offer them easy ways to withdraw consent at any time.

2.8. The GDPR states that you should ensure that the personal data you obtain is adequate and relevant; furthermore, it should be limited to what is necessary in relation to the purposes for which it was obtained. This means that when you are dealing with a constituent you should only obtain the absolute minimal amount of information required to assist. Additionally, the personal data should only

be shared with those individuals or organisations that is necessary to assist with the constituent's query for example when running council surgeries.

2.9. GDPR requires Councils to take prompt action when they become aware or suspect a personal data breach has occurred. In some cases, where the breach is likely to be a risk to an individual's rights and freedoms, the breach will need to be reported to the Information Commissioner (ICO). You must do this within 72 hours of becoming aware of the breach, where feasible.

2.10. If the breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR says you must inform those concerned directly and without undue delay.

2.11. If you become aware or suspect a personal data breach then you contact the Council's Data Protection lead, who will be able to guide you through the steps to take to contain and / or mitigate the breach and advise you as to whether you need to notify the ICO and / or the individual(s) effected.

3. Data Protection Principles

3.1. When personal data is processed, it should be guided by the following principles listed below, as set out in the GDPR, which require personal data to be:

• processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency).

• collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).

• adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data minimisation).

• accurate and where necessary kept up to date (Accuracy).

• not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).

• processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality).

3.2 Consent for one type of data processing does not give councils permission to do anything else with the personal data. e.g. a resident consents to be added to a newsletter mailing list and their details are used for a different purpose such as promoting the facilities of the council. Where councils collect consents, e.g. to be added to an email mailing list, these consents will need to be recorded. Councils may need several different consent forms (or elements within a single form) to cover different areas of data processing within the activities of the council.

4. Accountability & Responsibilities

4.1. Northleach with Eastington Town Council is the data controller, which determines how data is processed, and must pay a fee to the Information Commissioner's Office (ICO).

4.2. As the data controller, the council is responsible for establishing policies and procedures in order to comply with, and demonstrate compliance with, data protection law.

4.3. The council must therefore apply adequate resources and controls to ensure GDPR compliance as far as is practicable, including training and information.

4.4. The ICO has confirmed that small parish and town councils do not need to appoint a Data

Protection Officer (DPO). Notwithstanding the announcement, the council may decide to appoint a DPO.

4.5. The council must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles.

4.6. The council must produce the required documentation such as Privacy Notices, Data Retention Schedule, Records of Processing and records of Personal Data Breaches.

4.7. Where data is processed by a third party, such as a payroll provider, a data processor must be chosen that provides sufficient guarantees about its security measures; and reasonable steps taken to ensure that such security measures are in place to protect personal data.

4.8. Where there is uncertainty around a data protection matter, advice shall be sought from the council's Data Protection Officer (if applicable) and / or the ICO.

5. Role of Members of Council

5.1. Data protection laws affect councillors in three different capacities:

• as members of the council, and therefore subject to the same responsibilities as employees;

• when acting on behalf of a member of the public (casework); and

• personally, when the rights of data subjects apply.

5.2. Councillors will only seek access to personal data when this knowledge is essential for them to carry out official duties, or where the data subject has authorised the access (casework). The information should only be used for its intended purpose and deleted afterwards.

5.3. Where the councillor can take a copy of the personal information away from the premises, or where they have remote access to the information, the council may specify the steps to keep the information secure. For example, setting out rules about how personal information on a laptop or on paper should be stored securely and who can have access to it.

5.4. There is a duty to observe the data protection principles under Data protection. Act. Minutes cannot routinely record the names or other personal data of an individual unless this is for the performance of contractual obligations, statutory powers or functions of the council or if the individual consents. The minutes of a meeting should not ordinarily include personal data relating to members of the public who attended and spoke at the meeting.

5.5. A Council must apply the statutory data protection principles to its everyday internal administration, external communications and what is necessary for the performance of its statutory powers., functions and contracts. For example, the agenda and minutes of a meeting of a staffing sub-committee should not identify the name or other information about a member or of Staff.

6. Communicating Privacy Information

6.1. A 'Privacy Notice' and 'Cookie Policy' are available on the council website, which details who the council shares personal data with, how personal data is used and stored, the purposes for which personal data is used, and subject rights to their personal data.

6.2. The transparency requirements under the GDPR require councils to provide individuals with extensive information about how their personal data is collected, stored and used. This information

must be easily accessible, transparent and presented using clear and plain language. In practice, this means that councils will need to include more information in their privacy policies, as well as retaining more detailed records of their data processing activities in relation to their staff, customers and third parties.

7. Data Subject Access Requests

7.1. Data subjects have the right to receive a copy of their personal data held by the council. In addition, an individual is entitled to receive further information about their rights and how the council processes their personal data, including the categories, recipients, retention periods, and details of relevant safeguards where personal data is transferred outside the EEA.

7.2. The entitlement is not to documents per se (which may however be accessible by means of the Freedom of Information Act, subject to any exemptions and the public interest), but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

7.3. A response to each request will be provided within 30 days of the receipt of the written request from the data subject. Appropriate verification will be requested to confirm that the requestor is the data subject or their authorised legal representative. If the council cannot respond fully to the request within 30 days, the data subject will be kept fully informed of the progress of their request, and / or reasons for refusal and any procedure for appealing the decision.

7.4. Data subjects have the right to require the council to correct or supplement erroneous, misleading, outdated or incomplete personal data.

7.5. Personal data should not be altered, concealed, blocked or destroyed once a request for access has been received. The council will contact the ICO or Data Protection Officer (if applicable) for advice before any changes are made to personal data which is the subject of an access request.

8. Data Breaches

8.1. A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

8.2. If anyone (including a third party provider) knows or suspects a data breach has occurred, details of the alleged breach should be submitted immediately in writing to the Clerk.

8.3. The law requires that organisations report to the Information Commissioner's Office (ICO) any personal data breach where there is a high risk to the rights and freedoms of the data subject, such as identify theft, or serious damage to reputation.

8.4. Where there is doubt as to whether the breach is reportable, clarification shall be obtained from the ICO helpline on 0303 123 1113.

8.5. Data breaches will be reported using the ICO's online system: https://ico.org.uk/fororganisations/report-a-breach/.

8.6. The report shall be made as soon as possible and within 72 hours (daily hours not working hours) of becoming aware that an incident is reportable.

8.7. Where the breach is likely to result in a high risk to the rights and freedoms of individuals then those concerned directly will also need to be informed.

8.8. Evidence relating to personal data breaches must be retained, to enable the council to maintain a record of such breaches, as required by the GDPR.

9. Issue & Review

9.1. A copy of this policy will be brought to the attention of all employees and council members.

9.2. The council reserves the right to change this policy at any time without notice, so please check our website to obtain the latest copy.

This policy was approved by Northleach with Eastington Town Council on 18th September 2019.

Next Review due: September 2020

Glossary: The jargon explained:

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

Data controller is the person or organisation who determines the how and what of data processing.

Data processor is the person or firm that processes the data on behalf of the controller.

Data subject is the person about whom personal data is processed.

Personal data is information about a living individual which is capable of identifying that individual. E.g. a name, email addresses, photos.

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

Sensitive personal data is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.