Data Protection Policy

January 2020

Bolsover District Council

North East Derbyshire District Council

We speak your language

Polish
Mówimy Twoim językiem

French
Nous parlons votre langue

Spanish
Hablamos su idioma

Slovak
Rozprávame Vaším jazykom

Chinese
我们会说你的语言

If you require this publication in large print or another format please call: Bolsover District Council on 01246 242424 or North East Derbyshire District Council on 01246 231111

CONTROL SHEET FOR DATA PROTECTION POLICY

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	Data Protection Policy
Current status – i.e. first draft, version 2 or final version	Draft v2
Policy author (post title only)	Information, Engagement and Performance Manager
Location of policy (whilst in development)	S Drive
Relevant Cabinet Member (if applicable)	Portfolio holder for Corporate Governance (BDC) Portfolio holder for Council Services (NEDDC)
Equality Impact Assessment approval date	28/11/19
Partnership involvement (if applicable)	
Final policy approval route i.e. Joint Strategic Alliance Committee, Cabinet/Executive/Council	JSAC Executive (BDC) Cabinet (NEDDC)
Date policy approved	
Date policy due for review (maximum three years)	
Date policy forwarded to Performance (to include on Extranet and Internet if applicable to the public)	

DATA PROTECTION POLICY

1. Introduction

1.1. The processing of personal data is essential to many of the services and functions carried out by local authorities. North East Derbyshire and Bolsover District Councils ('the Councils') recognise that compliance with data protection legislation will ensure that processing is carried out fairly and lawfully.

1.2. The Data Protection Act 2018 (DPA) is an Act of Parliament which updates data protection laws in the UK. It is national law which complements the European Union's General Data Protection Regulation (GDPR 2016, applicable 2018). Together they form the framework for data protection law in the UK.

1.3. The Information Commissioner's Office (ICO) is the relevant supervisory authority for the UK. Set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

2. Scope

2.1 The policy is applicable to all employees, Elected Members, apprentices, agency workers, unpaid volunteers and those on work experience. In certain circumstances it will apply to contractors working for the Councils.

2.2 This policy applies to the collection and processing of all personal data as defined by the legislation as that of a 'natural person'. It covers all formats including paper, electronic, audio and visual formats. The policy will only deal with the personal data of a living person and does not apply to the data of a deceased person.

2.3 The policy applies to all employees working within Elections although the post of Electoral Registration Officer is registered, for the processing of elections data, with the Information Commissioner's Office separately.

2.4 Organisations who process data on our behalf, will have their own policy statements in respect to data protection.

3. Principles

3.1 The policy sets out the main requirements of the data protection legislation and how the Councils will comply. It is not a statement of how compliance will be achieved as this will be a matter for operational procedures and processes.

3.2 The policy will be made available to the public.

4. Data Protection Statement

4.1 Key Definitions (GDPR)

4.1.1 The GDPR applies to the processing of personal data that is wholly or partly by automated means or to the processing other than by automated means which forms part of, or is intended to form part of, a filing system. '**Filing system**' means any structured set of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis.

4.1.2 '**Personal data'** means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, a number, location data etc. This may also include online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers. Such identifiers may leave traces which combined with other information may be used to create profiles of the natural person and identify them.

4.1.3 The Councils are the **'Data Controller'** who determines the purposes and means of processing personal data. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.1.4 GDPR also applies to **'Data Processors'** who act on the controller's behalf and places further obligations on both parties. The 'Processor' means a natural or legal person, public body, agency or other body which processes personal data on behalf of the Councils.

4.2. Data Protection Principles

4.2.1. The following **principles** relate to the processing of personal data and set out the main responsibilities for the Councils under GDPR. Article 5 requires that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject. **(Lawfulness, fairness and transparency).**

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes. **(Purpose limitation)**.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. **(Data minimisation).**

(d) Accurate and where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having

regard to the purposes for which they are processed, are erased or rectified without delay**. (Accuracy)**.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this legislation in order to safeguard the rights and freedoms of the data subject. **(Storage limitation)**.

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. **(Security).**

4.3. Lawful Basis for Processing

4.3.1 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the Councils process personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform their official tasks.)

4.4 Special Category Data

4.4.1 Special category data is broadly similar to the concept of sensitive personal data under the 1998 Data Protection Act and covers information about an individual's:

- race;

- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

4.4.2 To process sensitive data the Councils must also satisfy a specific condition for processing under Article 9 of the GDPR.

4.4.3 This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. As such the Councils must ensure that adequate organisational and technical measures are in place to safeguard this data.

4.4.4 The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

4.4.5 To process personal data about criminal convictions or offences, the Councils must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.

4.4.6 Article 10 states that processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority. This means that the Councils must either process the data in an official capacity or meet a specific condition in Schedule 1 of the Data Protection Act 2018, and comply with the additional safeguards set out in that Act.

4.5 Data Subject Rights

4.5.1 The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The exercise of some of the rights is conditional upon the lawful basis for processing the personal data.

4.5.2 The Councils will ensure that information on how to exercise these rights is made easily available to individuals through its staff, website and appropriate documentation e.g. application forms.

4.5.3 Upon receipt of a verified request the Councils have one month to respond and cannot charge a fee to deal with a request under most circumstances.

4.5.4 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

4.5.5 The Councils must provide individuals with information including: purposes for processing personal data, retention periods for that personal data, and who it will be shared with. This is commonly referred to as 'privacy information'.

4.5.6 Articles 13 and 14 of the GDPR specify what information individuals have the right to be informed about. This information needs to be provided at the time the personal information is collected and must use clear and plain language. The information must be concise, transparent and easily accessible.

4.5.7 The Councils will provide privacy information in a variety of ways including published privacy statements, privacy notices on forms and posters and through its staff.

4.5.8 Individuals have the right to obtain the following from the Councils:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information – (this largely corresponds to the information that should be provided in a privacy notice).

This is commonly referred to as subject access.

4.5.9 An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).

4.5.10 Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The DPA 2018 says that we do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In these circumstances the Councils will need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights.

4.5.11 The Councils may seek to confirm the identity of an individual before responding to a request if needed.

4.5.12 The Councils will have in place operational processes for identifying and processing requests in line with legal requirements.

4.5.13 In some circumstances, the DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, the Councils may not have to comply with all the usual rights and obligations e.g. the right to be informed. The full list of exemptions are contained within Schedules 2-4 of the DPA 2018. Those covering crime and taxation and disclosures required by law or in connection with legal proceedings are the ones most likely to be relied upon by the Councils. The Councils consider the use of exemptions on a case-by-case basis and keeps records of its decisions.

4.5.14 Should any member of the public wish to make a complaint about the processing of their data by either of the Councils then they should use the Councils Complaints Procedure which is available on the website. The public also have a right to contact the Information Commissioners Office (https://ico.org.uk/) who are the supervisory authority for data protection matters under the legislation.

4.6 Accountability and Governance

4.6.1 Accountability is one of the data protection principles - it makes organisations responsible for complying with the GDPR and says that they must be able to demonstrate their compliance.

4.6.2 The Councils will put in place appropriate technical and organisational measures to meet the requirements of accountability including:

- adopting and implementing data protection policies;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests and implement measures to meet the 'data protection by design and default' approach;
- appointing a data protection officer at an appropriate level within the organisation and provide suitable resources to support the role.

4.6.3 Accountability obligations are ongoing. The Councils will keep its measures under review and update, where necessary.

4.7 Contracts

4.7.1 The GDPR makes written contracts between controllers and processors a requirement. (Rather than just a way of demonstrating compliance with the

seventh data protection principle (appropriate security measures) under the Data Protection Act 1998).

4.7.2 Contracts must include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the GDPR requirements, not just those related to keeping personal data secure.

4.7.3 The Councils will only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet GDPR requirements and protect data subjects' rights.

4.8 Security

4.8.1 The Councils are required to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998.

4.8.2 The Councils fully understand that poor information security leaves systems and services at risk and may cause real harm and distress to individuals. The Councils take their security obligations seriously.

4.8.3 The Councils recognise that information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help us demonstrate our compliance with other aspects of the GDPR.

4.8.4 The Councils will have technical and organisational measures in place to ensure a level of security appropriate to the risk of the personal data processing. These security measures will seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those we have authorised to do so (and that those people only act within the scope of the authority we give them);
- the data we hold is accurate and complete in relation to why we are processing it; and
- the data remains accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, we should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

4.8.5 The Councils technical measures will include physical and Information Technology (IT) security such as premises security, access control within the building including visitors, paper and electronic waste, keeping IT equipment, especially mobile devices, secure, and cybersecurity e.g. network and information systems, data, online and device security.

4.8.6 The Councils organisational measures will include this policy, its Information Security policy and internal guidance, provision of advice and a point of contact via the Data Protection Officer, developing a cultural awareness around information security, periodic checks to ensure that security measures remain appropriate and training.

4.8.7 All employees will receive initial and refresher data protection training appropriate to the personal data processing activities they undertake. The training will be mandatory for new employees and take place during their induction. Thereafter all staff who process personal data will be required to undertake refresher training every two years. Information security training is a requirement for every new starter using IT equipment and usually undertaken on the first day of work. Thereafter all staff who use IT equipment will undertake refresher training every two years. Elected Members will receive training on data protection and information security during their induction and thereafter as required.

4.9 Personal Data Breaches

4.9.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

4.9.2 Under GDPR (Recital 87) when a security incident takes place, we need to quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including notifying the Information Commissioner's Office (ICO) if required.

4.9.3 The duty requires the Councils to report certain types of personal data breach to the relevant supervisory authority (ICO) within 72 hours of becoming aware of the breach, where feasible.

4.9.4 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then the Councils must also inform those individuals without undue delay.

4.9.5 When notifying individuals the Councils will use clear and plain language to describe the personal data breach, provide contact details where more information can be obtained, describe any likely consequences of the personal data breach and the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

4.9.6 The Councils must also keep a record of any personal data breaches, regardless of whether we are required to notify the ICO. The Councils will document the facts relating to the breach, its effects and the remedial action taken.

4.9.7 The Councils will investigate whether or not the breach was a result of human error or a systemic issue and consider how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

4.9.8 The Councils will ensure that they have robust breach detection, investigation and internal reporting procedures in place. A risk based approach will be used to facilitate decision-making about whether or not we

need to notify the relevant supervisory authority (ICO) and the affected individuals.

4.10 International Transfers

4.10.1 The GDPR restricts the transfer of personal data to countries outside the European Economic Area (as individuals risk losing the protection of the GDPR).

4.10.2 A transfer of personal data outside the protection of the GDPR (referred to by the ICO as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA.

4.10.3 Personal data which the Councils process themselves is held on UK servers. When using an external provider for processing e.g. storing customer records, the Councils will use companies which have UK/EU/EEA based servers or ensure that any restricted transfer is undertaken in accordance with GDPR provisions.

5. Responsibility for Implementation

5.1 Keeping the policy under review and updating the policy is the responsibility of the Data Protection Officer for the Councils. The Senior Management Team are responsible for implementing this policy and the legislation in general.

5.2 Managers at all levels are responsible for ensuring that employees, agency workers, apprentices, unpaid volunteers and work placements for whom they are responsible are aware of and adhere to this policy. Managers are also responsible for ensuring that employees are updated in regard to any changes in this policy and receive regular training.

5.3 The Data Protection Officer assists the Councils to monitor internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority (ICO).