Ashfield
DISTRICT COUNCIL

Data Protection Protocol

January 2019

Contents

Ashfield District Council recognises its obligations to comply with the requirements laid down in the General Data Protection Regulation (GDPR) ((EU) 2016/679 and any national implementing laws, including the Data Protection Act 2018 (DPA).

1. Introduction

Ashfield District Council ('the Council') aims to ensure that personal information is treated lawfully and correctly. The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the Council deals and in achieving its objectives. This protocol sets out the basis on which the Council shall process any personal data from Individuals, staff and other parties from whom data is collected.

The Council, and therefore any person who handles personal data on behalf of the Council, fully endorses and adheres to the Data Protection principles set out in Article 5 of the GDPR and shall be responsible for, and be able to demonstrate, compliance with the principles outlined below:-

<u>The Six Data Protection Principles</u>

THE SIX DATA PROTECTION PRINCIPLES

Personal Information:

- shall be processed lawfully, fairly and in a transparent manner **(lawfulness, fairness and transparency)**
- shall be collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; **(purpose limitation)**
- shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; **(data minimisation)**
- shall be 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)**
- 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 in so far 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 to safeguard the rights and freedoms of the data subject (**storage limitation**)
- 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 (**integrity and confidentiality**)

2. Definitions

<u>Personal Data</u>

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, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For example, this will include:

- A name and address

- information attached to a reference number that could be used to identify someone directly or indirectly

- a company e-mail address if it includes a person's name

Personal data breach

Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed. Please see the Council's Data Breach Procedure.

Consent

Means any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.

Special categories of personal data

This is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation. (Previously known as Sensitive Data).

Processing

Includes:

- Any operation or set of operations, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration.
- Personal Information Request (previously known as a Subject Access Request). This is the right to access personal data by a data subject i.e. An individual.

Data Subject

This will be the person that we collect the data from. This includes Individuals, members of staff, members of the public and Councillors

3. Protocol Aim

To ensure the Council complies with all relevant legislation and good practice to protect all of the personal information that it holds.

4. Protocol Objectives

To achieve the overall aim the Council will:

- Provide adequate resources to support an effective approach to data protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise the Council's commitment to data protection.
- Compile and maintain appropriate procedures and codes of practice.
- Promote general awareness and provide specific training, advice and guidance to its staff at all levels to ensure standards are met
- Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary
- Monitor, report on and ensure compliance with this protocol, the GDPR and DPA through the Data Protection Framework, (for details of Framework agreement, see end of document – page 15), which will include training and be reported annually.

5. Processing of Information

The Council, through appropriate management controls will, when processing personal information about any individual, comply with the conditions set out below:

5.1 Observe fully the conditions regarding the collection and use of information and meet the Council's legal obligations under the GDPR and the Data Protection Act 2018.

5.2 Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

5.3 Ensure that the individual about whom information is held can exercise their rights under the GDPR and the DPA Act 2018 unless an exemption applies.
The rights include:-

- the right to be informed that processing is being undertaken
- the right to prevent processing in certain circumstances
- the right to correct, rectify, block or erase information, which is regarded as incorrect information
- the right of access to personal information
- the right to erasure
- the right to portability where applicable.

6. Processing of special categories of personal Information

The Council, through appropriate management controls will, when processing special categories of personal information about any individual, comply with the conditions set out below:

6.1 Observe fully the conditions regarding the processing of special categories of information as outlined in Article 9 and meet the Council's legal obligations under the GDPR and the DPA. In particular, Schedule 1 Part 4 of the DPA 2018 states that the Council must have a policy document in place which explains as below, the

procedures for securing compliance with the principles in Article 5 as outlined above. Please see the Appropriate Policy Document.

6.2 Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

7. Processing by Third Parties

Ashfield District Council as data controller will implement appropriate technical and organisational measures to ensure compliance with this protocol, the GDPR and DPA. This will include but not be limited to:

7.1 Undertaking a Data Protection Impact Assessment (DPIA) before selecting a third party processor where the processing is likely to result in a high risk to the rights and freedoms of Individuals.
7.2 Performing checks on potential third party processors to ensure their suitability for the role.
7.3 Entering into a contract with the third party which sets out the relationship, roles and responsibilities of the data controller and processor.
7.4 Ensuring that contracts comply with best practice and are recorded on the corporate contracts register by working with the procurement team in procuring the data processing contract.
7.5 Updating the Information Asset Register where appropriate.
7.6 Monitoring and contract management to obtain assurance that the third party is complying with its contractual and legal obligations, including data breach notifications.

8. Access to Personal Information

Ashfield District Council will process requests for access to personal information in line with the relevant sections of the GDPR and the DPA.

Individuals can request a copy of the personal data that the Council holds about them. Any staff member who receives a valid data protection request must forward it to the Council's Information Officers without delay to foi@ashfield.gov.uk. Responses to requests for information must be provided by the Information Officers only and normally within one month.

Complex and high volume requests can take longer to collect the information - Article 12(3) of the Regulations allows an additional two months on top of the statutory time scale of one month to deal with complex requests.
The Council is entitled to refuse to answer a request that is manifestly unfounded or excessive, particularly if the request is repetitive. Where a request is manifestly unfounded or excessive the Council will usually decline to comply with the request.
If in extreme circumstances the Council choose to comply with a request that the Council considers to be manifestly unfounded or excessive Article 12(5)(a) allows the Council to charge a reasonable fee taking in to account the administrative costs of complying with the request.
The Council will contact the individual (s) concerned and advise should the request fall under these categories.

The Information officers will action a valid request as follows:

- acknowledge the request and process the request;
- If more information is required this will be requested from the requester and the calendar month time for replying will commence once all the required information is received;

Requests from any external agency will be processed in accordance with the GDPR and DPA.

An appropriately qualified employee (normally a Solicitor) of the Council will ensure that any disclosure made without the consent of the data subject is done so in accordance with all DPA legislation and other relevant legislation, taking account of an individual's rights as enshrined in the Human Rights Act 1998.

9. Fair Obtaining/Processing

9.1 Individuals whose information is collected by the Council must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of an individual's personal information should take place unless reasonable steps have been taken to make that individual aware of that processing. This is generally in the form of a privacy notice. Individuals must also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information. The data subjects will also be informed of the purposes of the processing as well as the legal basis for processing. They should also be provided with the Data Protection Officer's details.
There are several basis for processing as set out below:

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

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

c) **Legal obligation**: the processing is necessary for you 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 you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests**: the processing is necessary for your 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 if you are a public authority processing data to perform your official tasks.)

NB. If consent is identified as the correct basis for processing, below is a brief checklist that will outline what you need to ensure is in place when you obtain consent to process personal data;

- Consent means offering individuals real choice and control.
- Consent should put the individual in charge and should be freely given
- Consent can't be a pre-condition in order to provide a service
- Consent requires a positive opt-in – using pre-ticked boxes or default consent is a big No!
- Consent must be specific for a purpose and granular, you can't use a one consent fits all approach.
- When giving consent to being contacted, individuals must be given the option to select methods of contact, be it post, email, letter, SMS, telephone
- Consent should be just as easy to withdraw as it is to give
- Keep a record of the consent given
- Consent needs to be refreshed at relevant and reasonable periods. These periods may differ depending on circumstances and advice should be sought
- To give consent the relationship between the giver and receiver must be equal. For example a single disabled homeless female with 2 children seeking housing assistance from the Council is not in an equal position to the Council. Consent therefore is not an appropriate basis to use to process her personal data.

9.2 Information must also be provided as to how long the information will be kept for, the rights that data subjects can exercise with regards to their data and information to enable data subjects to lodge a complaint with the Information Commissioners office if their rights are not met under the GDPR and DPA 2018.
For assistance in preparing a Privacy Notice, Officers should contact the Council's Legal service.

10. Data Uses and Purposes

10.1 All processing of personal data must be for a purpose that is necessary to enable the Council to perform its duties and services. Personal information should only be processed in line with those notified purposes.

Purposes will include the following:

- To allow the Council to be able to communicate and provide services appropriate to the Individual's needs, e.g. to be able to arrange suitable access arrangements where the Individual has mobility difficulties

- To ensure that the council meets its legal requirements, including obligations imposed under the Race Relations Act and Health and Safety Act

- Where necessary for the Council's Law Enforcement functions, e.g. licensing, planning enforcement, food safety, etc.

- Where the Council is legally obliged to undertake such processing for the purpose for which the data subject provided the information, e.g. processing information given on a benefit claim form, for the purpose of processing a

benefit claim, and to monitor the Council's performance in responding to the Individual's request.

- Where the processing is necessary for the Council to comply with its legal obligations, e.g. the prevention and/or detection of crime.

- To process financial transactions including grants, payments and benefits involving Ashfield District Council, or where Ashfield District Council is acting on behalf of other government bodies, e.g. Department for Works and Pensions.

- Where the Individual has consented to the processing

- Where necessary to protect individuals from harm or injury

- Where otherwise permitted under the GDPR and the DPA, e.g. disclosure to comply with legal obligations

- Ashfield District Council may also use an Individuals personal data, after it has been anonymised, to allow the statistical analysis of data to allow the Council to effective target and plan the provision of services.

- Safeguarding and promoting the welfare of children

- Providing human resources function for staff

10.2 All personal data should be regarded as confidential and be securely protected accordingly. This also applies when Council information is being processed at employee's homes. Employees should only remove personal information from a council office with the authority of their line manager, Director or the Chief Executive. A hard copy personal data removed from the Council Offices must be kept secure by the employee and not left in any vehicles or accessible to any family member at home. Any personal data held on laptops must be transferred to the Council network at the earliest opportunity and the original deleted. Council laptops and IT equipment must be kept secure, updated regularly and used in accordance with the Councils security policies. Any misuse, loss or unauthorised disclosures while the information is in their control may result in disciplinary proceedings. Information held by the Council must not be used for unauthorised non-Council purposes. If you become aware of any potential data breach, please refer to section 12 below, the Council's Data Protection Breach Procedure and follow the designated procedures accordingly.

10.3 Personal Information should only be disclosed to persons (internal and external) where their authority to receive it has been explicitly established, e.g. where the information is required by the police for the prevention and detection of crime, or a relevant Information Sharing Agreement is in place, or they have consent.

10.4 Information processed should not be excessive or irrelevant to the notified purposes.

10.5 Information must be held only for so long as is necessary for the notified purposes, after which it should be deleted or destroyed in accordance with the Council's Retention and Disposal Schedule

10.6 Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

11. Data Incident Reporting/ Data Breach

11.1 Employees must notify the Data Protection Officer of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after becoming aware of the potential breach by contacting DPO@ashfield.gov.uk

11.2 Any reported data incident will be investigated appropriately with the relevant stakeholder(s) and actions taken as necessary.
11.3 If a member of the public wishes to report a potential incident, they can do this by contacting the Data Protection Officer directly on 01623 450000 or by e-mailing DPO@ashfield.gov.uk

11.4 Serious suspected Personal data breaches will be notified to the Information Commissioner's Office where appropriate within 72 hours of the incident. Only the Council's Data Protection Officer will report suspected breaches. All staff members will follow this guidance, the Data Protection Breach procedure and the Information Commissioners Office guidance.

12. Records of processing activities

12.1 In order to be able to properly and effectively comply with our obligations under the GDPR and the DPA 2018, the Council needs to fully understand what information it holds and where this information is kept. We also need to consider how we keep this information up-to-date and how we know when to dispose of it. We also have to record the Legal Basis that applies to the processing of the personal data.

12.2 The Council shall maintain an Information Asset register which shall document what personal data comes into the council, leaves the council, how the data is held, retention periods, who the information is shared with and the legal basis for processing, for information about the Legal basis for processing, please see guidance note – Lawful Bases for Processing Personal Data (see appendix 1).

12.3 The IAR will be reviewed annually. Departments are responsible for ensuring their information contained in the IAR is accurate and up to date.

13. Data Security

13.1 The Council is obliged to ensure that all appropriate technical and organisational measures are taken to safeguard against unauthorised or unlawful processing of personal information and against the accidental loss, damage or destruction of personal information.

13.2 All personal information must be kept secure, in a manner appropriate to its sensitivity and the likely harm or distress that would be caused if it was disclosed unlawfully. To ensure that an appropriate level of security is afforded to all information the Councils' Information Security policy will be adhered to at all times.

13.3 Everyone managing and handling personal information will be appropriately trained to do so and this will include appropriate refresher training every year.

13.4 All members of staff have a duty to follow this Protocol and associated procedures and to co-operate with the Council to ensure that the aim of this Protocol is achieved.

13.5 Disciplinary action may be taken against any member of staff who fails to comply with or commits a breach of this Protocol. Everyone has a responsibility to ensure that personal data is only used for lawful purposes and to ensure that data is kept secure and not accessed for personal reasons. It is a criminal offence to misuse personal data, which may result in a criminal investigation/prosecution against the individual (staff member) concerned.

13.6 It is the duty of individual members of staff to ensure that personal information held by them is dealt with in accordance with the GDPR and the DPA.

13.7. Suitable measures should be taken to ensure that any processing of personal data carried out by a third party on behalf of the Council complies with the principles of the GDPR and this Protocol. Similarly, when the Council is processing personal information on behalf of a third party it will need to demonstrate that the information is subject to the same standard of care.

13.8 No data should be shared with either an internal department or external body without first establishing the Legal basis for sharing it, if unsure speak to Legal. Advice should always be sought from Legal services before any data is shared externally.

This Data Protection Protocol should be read in conjunction with the following documents which make up the Data Protection Framework:

- Records, Retention & Disposal Policy (ADC Retention Schedule)
- Corporate Records Management Best Practice Corporate Records Management Best Practice
- Security Policies
- IT Acceptable Use policy
- Data Protection Breach Procedure
- Personal Information Requests Guidance which can be found on the Council's Data Protection Act page and Personal Information Requests application form
- Privacy Statement (www.ashfield.gov.uk/privacy)
- DPIA guidance
- Data Quality Strategy 2018
- Appropriate Policy Document.
- Guidance notes – which can all be found on the GDPR page on the Intranet, as follows:

1. Privacy Notice Update
2. Do you rely on consent in order to process individuals' personal data?
3. Do you use Mailchimp to manage a mailing list or contact schedule?
4. Amended Terms and Conditions for Procurement Exercises

The following useful Briefing Notes can also be found on the Council's Intranet:

- Overview
- Key Differences
- Lawful Bases
- Mailing Lists
- Criminal Offences