Data Protection Policy

Title	Data Protection Policy
Document version	1.3
Release date	06/01/2020
Author	Tony Smith
Consultation	• Cabinet member for governance • Corporate Management Team • Legal • Policy • Trade Unions • Arvato
Equality Impact Assessment	Please refer to the Information Assurance Equality Impact Assessment.
Review date	1 year from publication
Version History	1.0 –02/05/2018 - Published 1.1 – 09/07/2019 - Reviewed by Tony Smith. Removed reference to councillors paying ICO fee. Added DBS appendix. 1.2 – 27/07/2020 - Reviewed by Rachael Beck. No changes. 1.3 – 31/12/2020 – Reviewed by Rachael Beck following Brexit changes. References to EU GDPR changed to UK

Contents

Policy statement

It is council policy that all personnel will take responsibility for managing information in accordance with this Data Protection Policy.

This policy outlines how Chesterfield Borough Council (referred to as "the council" in this document) will protect its information assets by informing users of the data protection requirements that directly apply to them in their day to day handling of information to ensure its information is secure, allowing the information to be used effectively for delivering its services and data subject's rights are upheld.

Scope

All personnel, physical locations, information assets, supporting assets and 3rd parties as required.

Information assets in scope

All records created and held in all physical and electronic formats, including, but not restricted to:

- Paper
- Electronic / digital documents, including scanned images, databases and spreadsheets
- E-mail and voice mail
- Information held in blogs, wikis and discussion threads, and in other social media when used for business purposes, such as Twitter
- Visual images such as photographs
- Microform, including microfiches & microfilm
- Information stored on removable media, such as audio and video tapes, memory sticks, CDs, DVDs and cassettes
- Published web content (Intranet/Internet/Extranet)

Objectives

The main objectives of this policy are:

a) To uphold the rights of the data subject
b) To ensure everyone handles council information in accordance with the council's information assurance policies and guidelines
c) To manage risks to protect the confidentiality, integrity and availability of the information assets of the council affording additional protection to sensitive information

d) To comply with relevant legislation including the Data Protection act 2018 and the UK General Data Protection Regulation
e) To comply with contractual security requirements
f) To follow (where appropriate) information security best practices
g) To provide accountability to those people who protect the Council's information assets and supporting assets
h) To support efficient working practices

Roles & responsibilities

All personnel have a duty to ensure the council's information assets and information systems are used securely and efficiently.

Policies

1. Data Protection Principles

1.1. The council will ensure that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
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
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
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

2. Lawfulness of processing personal data

2.1. The council will ensure that at least one of the following lawful conditions applies to each category of personal data processed for each purpose for processing:

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

3. Processing criminal offences data

3.1. The council will only process personal data relating to criminal convictions and offences if a lawful basis for processing personal data (above) has been identified and processing is being performed either:

a) in an official capacity or
b) we have specific legal authorisation

3.2. The council will not hold a comprehensive register of criminal convictions unless we are doing so in an official capacity as established in law

3.3. The council will process DBS (Disclosure and Barring Service) certificate information in accordance with the DBS Code of Practice requirements (see Appendix A)

4. Lawfulness of processing sensitive personal data

4.1. The council will ensure that the following special categories of personal data have a lawful basis for processing:

a) race
b) ethnic origin
c) politics
d) religion
e) trade union membership
f) genetics
g) biometrics (where used for ID purposes)
h) health
i) sex life or

j) sexual orientation

4.2. The council will ensure that at least one of the following lawful conditions applies to each category of sensitive personal data processed for each purpose for processing:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes…
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent…
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim…
e) processing relates to personal data which are manifestly made public by the data subject…
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity…
g) processing is necessary for reasons of substantial public interest…
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care…
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…

5. Data Subjects Rights

5.1. The council will maintain standard operating procedures to ensure the individual rights of data subjects are upheld namely:

a) The right to be informed
b) The right of access (subject access requests)
c) The right to rectification
d) The right to erasure (right to be forgotten)
e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling

5.2. Individual rights requests will aim to be resolved within one calendar month and free of charge

5.3. The council will maintain and provide privacy information to data subjects

6. Conditions for processing of personal data outside the United Kingdom

6.1. The supervisory authority's guidance will be followed to ensure that any personal data processed outside of the United Kingdom has an adequate level of protection and is in accordance with the law

7. Accountability and Governance

7.1. The council will maintain the designation of a Data Protection Officer

7.2. The council will maintain documentation for 'records of processing activities' of personal data

7.3. The council will maintain an 'Information Security Policy' to ensure appropriate technical controls are in place to protect personal data

7.4. The council will conduct data protection impact assessments where appropriate

7.5. The council will maintain suitable data protection training to staff and ensure it is part of their learning and development programme

7.6. The council will maintain its annual payment of the data protection fee to the supervisory authority (the Information Commissioner's Office) (ICO))

7.7. The council will follow the supervisory authority's guidance to ensure that its processing of personal data is in line with the supervisory authority's best practices

7.8. The council will ensure contracts and data sharing agreements are in place to ensure all parties understand their responsibilities and liabilities for processing personal data

8. Personal data breaches

8.1. The council will report any relevant data breaches within 72 hours of becoming aware of the breach to the supervisory authority

8.2. The council will also inform data subjects without undue delay if a breach is likely to result in a high risk of adversely affecting the data subject's rights and freedoms

8.3. The council will maintain a log of any personal data breaches

9. Children’s personal data

    9.1. Particular attention will be afforded to processing children’s personal data in accordance with the supervisory authority’s guidance

Appendix A - Handling of DBS certificate information Guidelines

These guidelines cover the secure storage, handling, use, retention and disposal of Disclosure and Barring Service (DBS) certificates and certificate information.

As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, Chesterfield Borough Council complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

It also complies fully with its obligations under the Data Protection Act 2018 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information.

Storage and access

Certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling

In accordance with the law, certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Once the inspection has taken place the certificate should be destroyed in accordance with the code of practice.

Usage

Certificate information is only used for the specific purpose for which it was requested and for which the applicant’s full consent has been given.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints.

If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the Data Protection and Human Rights of the individual before doing so.

Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding.

While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. general waste bin or confidential waste sack).

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

Acting as an umbrella body

Before acting as an umbrella body (an umbrella body being a registered body which countersigns applications and receives certificate information on behalf of other employers or recruiting organisations), we will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of certificate information in full compliance with the code of practice and in full accordance with this policy.

We will also ensure that any body or individual, at whose request applications for DBS certificates are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.