Borough Council of
King's Lynn &
West Norfolk

Data Protection Policy

Revised November 2023

Owner		Laura Botten, IGO		
Responsible Person *(non-substantive updating)*		Alexa Baker, DPO		
Review Cycle *(1 to 5 years)*		Every 2 years or changes to legislation	**Next Review Date**	November 2025
Last Impact Assessment (IA) Date			**Next IA Date**	
Date initially approved by Cabinet		tbc		
Published to *(internal, external or both)*		Both		
Stakeholders consulted? *(please tick to confirm)*		**Yes**		**No**	
Policy Published to	**Policy will be published on InSite and publicised via internal Staff Update.**			

Revision Record		
Rev. No.	**Date of Issue**	**Reason for Revision**
0.01	May 2018	Introduction of GDPR
0.02	Nov 2022	Review period / following UK GDPR
0.03	Nov 2023	Review period

Contents Page

1. Introduction

1.1 The Borough Council of Kings Lynn & West Norfolk ("The Council") supports the aims and provisions of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 and seeks to ensure compliance with the requirements of this legislation ("the legislation").

1.2 The Borough Council is the data controller. Electoral Services at the Borough Council of Kings Lynn & West Norfolk is also a data controller. This Data Protection Policy applies to both these data controllers. Elected Members act in their role within the Council and where they do, this policy applies to them. Sometimes elected Members are data controllers in their own right as well. In that situation, they will control how they implement the processing of data under the legislation.

1.3 This Policy sets out how we handle the personal data of our service users, suppliers, employees, workers and other third parties. It provides information and guidance to support the council's compliance with data legislation.

1.4 This Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject and provides information and guidance to support Council work and activities when dealing with personal information. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy.

2. Purpose

2.1 The purpose of this policy is to ensure that the provisions of the DPA and the UK GDPR are complied with and to protect the personal data of individuals.

2.2 This policy will assist the Council to comply with the requirements of the DPA and the UK GDPR. It will also seek to increase awareness of the rights of an individual under data protection legislation. Other relevant legislation can be found at **Appendix D**.

2.3 The data protection principles set out in the UK GDPR are principles which protect the personal data of individuals. As such, these principles are of paramount importance and must be followed (**Appendix A**). Information about legal basis for processing personal data is at **Appendix B** and a glossary of key terms can be found at **Appendix C**.

3. Why is Data Protection and Information Management important?

3.1 Information management is the process of collecting, storing, managing, and maintaining information assets in all their forms. Information governance is concerned with protecting the assets of the organisation from potential loss, loss of integrity, destruction or theft. They are inextricably linked; one does not exist without the other.

3.2 IT systems, filing cabinets and indexes may all contain important business information assets. Their confidentiality, integrity, availability and suitability are essential in maintaining the Council's effectiveness, efficiency and legal compliance. Information governance provides an enabling mechanism for sharing information whilst ensuring the protection of the data/information.

3.3 An Information Asset is "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles." Information is commonly defined as an asset. Information may exist in many media such as electronic or hard copy. It can be stored on computers, transmitted across networks, printed out, written down on paper or spoken in conversation. The Council owns a variety of information assets which are maintained by different services. It is the responsibility of services to ensure the security, availability, and usefulness of their information.

4. Aims

4.1 This policy aims to assist staff and other relevant persons in meeting their data protection obligations under the UK GDPR and related data protection legislation.

4.2 The Data Protection Act 2018 ("the DPA"), and the UK GDPR set out a framework of rights and duties which safeguard personal data.

Personal data is information relating to a living individual who can be identified from the data. The legislation balances the legitimate needs of organisations to collect and process data against the rights of individuals to respect for their rights to control their personal data and their privacy.

4.3 In addition to the DPA and the UK GDPR, several pieces of legislation deal with the rights and responsibilities of individuals and organisations in relation to personal data. A list of relevant legislation, though not exhaustive, can be found at **Appendix D**.

4.4 The Council recognises the importance of personal data to its business and the importance of respecting the information and privacy rights of individuals. This Policy sets out the principles which it will apply to the processing of personal data so that the Council not only safeguards one of its most valuable assets but also processes personal data in accordance with the law.

4.5 **It is the responsibility of all of the Council's employees, Members and any person holding or processing personal data on behalf of the Borough Council to assist with the implementation of this Policy.** In order to help employees comply, the Data Protection Officer arranges the provision of training of staff and produce guidance documents. An e-learning module, Data Protection, is available on the Learning Hub for mandatory completion. Employees should familiarise themselves with this Policy and guidance, complete training and apply the provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which can be a disciplinary matter and could ultimately lead to the dismissal of staff. Serious breaches could also result in personal criminal liability. This policy continues to apply to individuals even after their relationship with the Council ends.

4.6 In addition, a failure to comply with this Policy could expose the Council to enforcement action by the Information Commissioner or to complaints or claims for compensation from affected individuals. There may also be negative publicity and reputational damage as a result of any breach that is made public.

5. Key Features of the Data Protection Legislation

5.1 The DPA and the UK GDPR set out data protection principles. This legislation governs the processing of personal information both by way of manual records and computerised information. Individuals have

rights within the legislation, which includes a certain control over how their information is handled.

Here are some of the key features of the legislation:

a) All personal data must be handled in accordance with the Data Protection Principles (Appendix A).

b) Individuals ("data subjects") have rights surrounding how their information is handled. This includes the right to be informed about how and what of their personal information is being processed; the right to request access to that information ("a subject access request"); the right to request that inaccurate or incomplete data be rectified; the right to erasure or restriction of the processing of their information, including profiling, in certain circumstances. In addition, individuals can object to automated decision making and also have rights to object to profiling and rights relating to data portability.

c) Processing of data (including special category data and criminal offence data) must be done under a lawful basis in a fair and transparent manner. The conditions for processing personal data can be found at **Appendix B** along with further guidance on the processing of special category data and criminal offence data.

d) The principle of accountability of data controllers is of utmost importance. Suitable and sufficient systems, procedures, documents and training must be in place to demonstrate compliance with the data protection legislation.

e) Data protection impact assessments (DPIAs) are carried out where appropriate as part of the design and planning of new projects. Guidance relating to completion of DPIAs can be found at **Appendix E.**

f) Data controllers must have written contracts in place with all external bodies that process Council data. Data processors should only be appointed where they can provide sufficient guarantees that the requirement of the legislation will be met, and data subjects will be sufficiently protected.

g) Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the Borough Council becoming aware of the breach. Where the breach is likely to result in a high risk to the individual, those individuals are to be notified directly.

h) The Information Commissioner is responsible for regulation and can take action against organisations who do not comply with the requirements. In serious cases, the Information Commissioner can issue fines and prosecute those who commit offences under the legislation.

6. Roles and Responsibilities

6.1 All staff and relevant persons have a role in implementing this policy. There are some members of staff with key roles.

6.2 Data Protection Officer

The Data Protection Officer ("DPO") has a degree of autonomy within the Council, and is responsible for advising the Council, including its senior leaders, of its obligations under the legislation. The DPO is designated on the basis of professional qualities and expert knowledge of data protection law and practice. The DPO monitors compliance, raise awareness, and ensures training for staff to enable them to lawfully comply with processing operations. The DPO is the contact point with the Information Commissioner's Office for information law related issues and in the event of data breach. The Council must provide the DPO with the necessary resources and access to personal data and processing operations to enable them to perform their role and to maintain their expert knowledge of data protection law and practice. The DPO works within the legal department of the Council and is assisted by officers in dealing with requests and queries from individuals relating to their information rights as well as queries from members of staff and relevant persons. In the event of a breach or suspected breach of personal data, the DPO (and IAO) should be informed at the earliest opportunity by completing a data breach incident report form - https://forms.west-norfolk.gov.uk/DATABREACHINCIDENTREPORTFORM/launch

Please contact the DPO with any questions about the operation of this Policy or the UK GDPR or if you have any concerns that this Policy is not being or has not been followed.

6.3 Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) is a senior officer of the Council and has responsibility for ensuring the effectiveness of the Council's information risk management and managing information risks and incidents.

6.4 Information Asset Owners

Assistant Directors are “Information Asset Owners” (“IAO”). They are responsible for ensuring operational compliance with this policy within their own departments. IAOs keep and maintain a register of information collected by their service area. This information is held in a document called an ‘Article 30 record’, and includes details of personal data collected and held, why it is collected and who it may be shared with. The IAOs will report to the SIRO.

6.5 **Information Asset Assistants**

The day-to-day maintenance of this register will be by Information Asset Assistants (“IAA”). Each service will have at least one IAA. The IAA is also the contact point within the department where access to information requests is directed to and co-ordinated by.

6.6 **Information Governance Officer**

The IGO supports the Data Protection Officer in ensuring the council is compliant with the General Data Protection Regulation (GDPR) and all Information Governance legislation and regulatory frameworks. They also process, record, and facilitate responses to all Freedom of Information and Data Protection requests, liaising with Directorates to ensure compliance with all aspects of the legislation, and liaising with the Information Commissioners Office as required.

7. The rights of a data subject and Subject Access Requests (SARs)

7.1 Data subjects can make a request to know if the Council holds their personal data and for a copy of such. These are referred to as “subject access requests” (SARs). The Council will require proof of identity of the requestor. Any such request must be made in writing, but the Council will make reasonable adjustments in appropriate cases. There is a wider obligation to make information available via the Freedom of Information Act and Environmental Information Regulations. This is covered by the Council’s FOI/EIR procedures (see section 9).

7.2 In addition to a right to access personal information, data subjects have the following rights:

a) A right to rectification (if the data held is inaccurate)

b) A right to erasure in certain circumstances (“the right to be forgotten”)

c)A right to restrict processing of their personal data in certain circumstances

d)A right to data portability (a packaged transfer of data from one data controller to another)

e) A right to object to profiling; direct marketing and/or automated decision-making

7.3 The Council is committed to dealing with requests for information promptly and within one calendar month. However, where the request is complex, this response period may be extended by up to two extra calendar months.

7.4 The Council will respond to the request. If a request is refused, it will give a reason for the refusal and provide details of how the requestor can complain.

8. Sharing information

8.1 Whilst the legislation requires the Council to keep personal information of others secure and not to disclose it to a third party, there are some exemptions, which allow for such. In appropriate cases, and where permitted by law, the Council may share information where it is in the public interest to do so, for example, for the prevention or detection of crime. The Information Commissioner's website provides useful guidance notes, which may assist the Council in considering how it shares and discloses information.

8.2 Where personal data is stored and processed about employees of the Borough Council, the sharing of such data must also be in accordance with the data protection principles. Information rights legislation has introduced greater expectations of transparency in the affairs of public authorities, for example, disclosure may be acceptable if the data relates to the performance of public duties or the expenditure of public funds by senior employees. Senior employees should expect their posts to carry a greater level of accountability, since they are likely to be responsible for major policy decisions and expenditure of public funds. However, the Council will have regard to the Information Commissioner's guidance and its own privacy notices when considering whether personal data can be shared.

8.3 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

8.4 This policy applies to all personal data held by the Council, regardless of how it is collected, recorded, and used and whether it is on paper records or electronic records, including the information gathered on

CCTV (closed circuit television systems) and held within non-corporate communications channels (NCCCs), at whatever location used by or on behalf of the Council.

9. Freedom of Information Requests (FOI)/ Environmental Inquiry Regulations (EIR)

9.1. Since January 2005 the Freedom of Information Act (2000) (FOIA) and the Environmental Information regulations (2004) (EIR) have given the public rights of access to information held by public authorities.

9.2 We will meet its legal obligations to respond to all request for information and will supply that information, subject to the limited exemptions / exceptions as specified by law.

9.3 Requests can be made by anyone regardless of their age, nationality, location, profession, motives, or history. Requests will be dealt with in an applicant blind manner, i.e. each will be treated equally regardless of who is making the request. The exception to this is where an individual requests information about themselves.

9.4 Requests can be for any information that is held by the council, regardless of how the information was produced or obtained. It includes information about or obtained from other organisations including contracts, partnership information and agreements.

9.5 A request under FOI must be:

- Written (Letter, email, or fax acceptable)
- Legible
- Provide a name
- Provide an address for response (email acceptable)
- Describe the information sought sufficiently for the Council to identify it.

9.6 EIR does not require the request to be made in writing; however, such requests must be recorded and logged. For FOI and EIR, the requestor does not have to mention any legislation in their request and they are not required to know our process, procedures, and jargon to describe the information requested.

9.7 All requests will be logged and responded to in accordance with our procedures and supporting guidance for handling requests. Guidance notes are available here - Officer Guidance FOI EIR V0.01 July 2023.docx.

9.8 We will monitor the requests made to identify information regularly sought by the public. The Council will pro-actively publish information requested.

9.9 We will not create new information to respond to a request. However, we will provide related information and provide advice to assist the requestor obtain the information sought.

9.10 Requests should be made/forwarded to freedom.information@west-norfolk.gov.uk. Heads of Service, Assistant Directors and Directors are responsible for ensuring that their service areas comply.

10. Confidentiality and security

10.1 The Council recognises that everyone has a responsibility within the organisation to promote good data protection management.

10.2 Employees and relevant persons must not access, copy, alter, interfere with, or disclose personal data held by the Council unless permitted to do so under the data protection legislation.

10.3 Individuals that process personal data must comply with the Council's security measures to safeguard personal data as outlined in the Council's ICT Security Policy - Corporate E-Mail Policy (west-norfolk.gov.uk)

10.4 Any employee, Member or other person who becomes aware of a weakness in the Council's data protection procedures or who becomes aware of any breach of the policy should report the concern to their line manager at the earliest opportunity and to the DPO/IGO or the SIRO without delay. A breach procedure has been produced for IAO's and there is a data breach incident e-form on the intranet - https://forms.west-norfolk.gov.uk/DATABREACHINCIDENTREPORTFORM/launch

10.5 Where there has been a data breach, the Council has a duty to find out what data has been disclosed, lost, or stolen; to mitigate the loss and to take steps to notify persons affected where appropriate. There is also a general duty to contact the Information Commissioner's Office within 72 hours. Further information is available from the DPO and the IGO, the Council's breach procedure document and via the ICO website.

11. Register of Information Assets

11.1 The UK GDPR requires us to keep full and accurate records of all our data processing activities. The Council holds and maintains a register of information assets. The Information Asset Owner is responsible for compiling and maintaining the record of information assets for their department, aided by one or more Information Asset Assistants. These records are also referred to as Article 30 Registers and there is a process in place to ensure these are reviewed and updated accordingly. Each data controller must pay an annual fee to the Information Commissioner's Office (ICO).

12. Retention and Publication Scheme

12.1 The Council has a data retention and disposal policy which informs of the period for which documents and personal information is retained.

12.2 The Council informs individuals of its privacy policy via its website and will provide copies in such other reasonable format on request.

12.3 The Council has adopted the Information Commissioner's model publication scheme. Wherever possible information on the publication scheme will be published on the internet. Other information included on the scheme will be provided by services within 5 days. These requests will not be logged as FOIA / EIR requests. A guide to the publication scheme will be maintained and published by the Corporate Governance team.

13. Data Protection Impact Assessment (DPIA)

13.1 Article 25 of the GDPR makes privacy mandatory to consider and undertake in certain circumstances. Putting privacy at the heart of a project is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether. A DPIA will make sure that all risks and issues are considered and mitigated.

13.2 On Insite, there is guidance and the relevant documents to help determine whether a DPIA is needed. Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

14. Data Breaches

14.1 GDPR Article 4 (12) states that a breach of security is an occurrence when there is an **accidental** or **unlawful** destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. What to do if there is a breach of personal Data – April 2023 provides guidance on what should be reported and how.

14.2 A breach can occur in many ways, but may be described as:

- Loss or theft of information / data held in paper or electronic form
- Loss of equipment on which data is stored
- Inappropriate access controls or failure of these controls allowing unauthorised access, use or changes to information / data.
- Equipment failure.
- Human error e.g. overwriting data.
- Unforeseen circumstances such as flood / fire/ explosion.
- Hacking attack.
- “Blagging” – obtaining information by deception.
- Accidental or deliberate disclosure of information to a third party.

14.3 However a breach occurs, steps must be taken to minimise the impact of the loss and measures taken to prevent re-occurrence. We must consider all possible adverse effects on individuals which can result material or non-material damage. The definitions of this are:

- loss of control over personal data
- limitations of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of Pseudonymisation
- damage to reputation
- loss of confidentiality

14.4 If there is a risk of such effects taking place then we will need to report to the ICO or face corrective measures. If there is a high risk, then we must also inform the subject.

14.5 The following steps must be taken on discovery of a security breach or weakness:

1. Report the breach to appropriate line management and the Corporate Governance Team via the web form immediately. The IGO/DPO will need to know:

- The nature of the breach (what has happened)

- What information has been affected (sensitivity and volume of the information)
- What immediate action has already been taken in response to the breach

2. Reporting member of staff to ensure that any breach is contained as far as possible and where possible that any personal data is recovered.

3. The Corporate Governance Team will gather any further details required at this stage to decide on whether to begin notifying the ICO of the breach. If a breach is serious enough to be reported to the ICO, this must be done by the Corporate Governance team within 72 hours of the breach occurring.

4. The Corporate Governance Team will provide advice on whether it is appropriate to notify stakeholders (including the affected individuals, Communications Team, the SIRO) and agree actions with the service to attempt to prevent similar incidents occurring in the future. Recommendations made in response to breaches will be reported annually.

14.6 Article 33 of GDPR states that there is a requirement to notify breaches to the ICO where it is likely to result in a **risk** to people's rights and freedoms.

14.7 Article 34 of GDPR states that there is a requirement to communicate a breach to data subjects where it is likely to result in a **high risk** to people's rights and freedoms. The impact of the breach will be assessed by Corporate Governance team.

15. Further Information, Enquiries and Complaints

15.1 The Council's DPO is the first point of contact on any of the issues mentioned in this Policy. The DPO will be responsible for dealing with all individual and external enquiries. All service areas will have a nominated data protection contact officer, also known as the Information Asset Assistant (IAA) to create a network to assist the Council's DPO when responding to subject access requests and other information rights requests.

Data Protection Officer
Borough Council of King's Lynn & West Norfolk
Kings Court
Chapel Street
King's Lynn
Norfolk PE30 1EX

15.2 Where a person wishes to raise an issue or complaint about how their personal information is, or has been, processed, they should in the first instance be directed to the DPO.

Information Commissioners Office

The ICO is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken.

The ICO contact details are as follow:

www.ico.org.uk

Helpline: 01625 545 745.

APPENDIX A

The Personal Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR which personal data to be:

a) Personal data shall be processed lawfully, fairly & transparently (‘lawfulness, fairness and transparency’)

b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’)

c) Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)

d) Personal data 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’)

e) Personal data shall be 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 (‘storage limitation’)

f) Personal data shall be processed in a manner that ensures appropriate security of the personal data, including against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)

APPENDIX B

Processing personal data

A. Conditions for processing personal data

The basis for processing personal data must be lawful. At least one basis from the list below must apply whenever the Council processes personal data:

a) **Consent** – the individual has given clear consent for the Council to process their personal data for a specific purpose (Note: consent can be withdrawn at any time).

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

c) **Legal obligation** – the processing is necessary for the Council to comply with the law.

d) **Vital interests** – to protect the vital interests of the data subject.

e) **Public task** – the processing is necessary for the Council to perform a task in the public interest or for the Councils official functions, and the task or function has a clear basis in law.

f) **Legitimate interests** – but cannot be used for processing carried out by public authorities in the performance of their tasks.

B. Processing special category personal data

The UK GDPR gives extra protection to special category data. Special category data is:

a) Personal data revealing racial or ethnic origin;

b) Personal data revealing political opinions;

c) Personal data revealing religious or philosophical beliefs;

d) Personal data revealing trade union membership;

e) Genetic data;

f) Biometric data;

g) Data concerning health;

h) Data concerning a person's sex life; and

i) Data concerning a person's sexual orientation.

If you are processing special category data, you need to identify both a lawful basis for processing (above) and a special category condition for processing in compliance with Article 9 of the UK GDPR. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability. It is also advised that a Data Protection Impact Assessment is completed and documented.

There are conditions for processing special categories of personal data, set out in Article 9 of UK GDPR and are summarised:

a) The data subject has given explicit consent, or

b) It is necessary for employment, social security, or social protection law*

c) It is necessary to protect life or where an individual is physically or legally incapable of giving consent

d) It is carried out during legitimate activities by certain not for profit organisations where it relates to specific persons

e) Where the personal data is manifestly made public by the individual

f) It is necessary for the establishment or defence of legal claims

g) It is necessary for reasons of substantial public interest*

h) It is necessary for purposes of preventative or occupational medicine and reasons relating to the provision of healthcare*

i) It is necessary in the interest of public health*

j) It is necessary for archiving purposes in the public interest or for scientific or historical research. *

*Additional conditions will need to be met before processing.

C. <u>Processing Criminal Offence Data</u>

The UK GDPR gives extra protection to personal data relating to criminal convictions and offences or related security measures, referred to as criminal offence data. This covers a wide range of information about:

a) Criminal activity;

b) Allegations;

c) Investigations; and

d) Proceedings.

It may also include:

a) Unproven allegations;

b) Information relating to the absence of convictions; and

c) Personal data of victims and witnesses of crime.

It also covers related security measures:

a) Personal data about penalties;

b) Conditions or restrictions placed on an individual as part of the criminal justice process; or

c) Civil measures which may lead to a criminal penalty if not adhered to.

If you are processing data about criminal convictions, criminal offences, or related security measures, you need both a lawful basis for processing (above), and either 'official authority' or a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability. It is also advised that a Data Protection Impact Assessment is completed and documented.

As a public authority, it is our responsibility to identify the specific law that gives the official authority requirement to process criminal offence data.

If official authority is not relevant for the purposes of processing criminal offence data then a separate condition must be met as set out in Schedule 1 of the DPA 2018.

The 28 conditions, which are available for processing of criminal offence data, are set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018:

1. Employment, social security, and social protection

2. Health or social care purposes

3. Public health

4. Research

6. Statutory and government purposes

7. Administration of justice and parliamentary purposes

10. Preventing or detecting unlawful acts
11. Protecting the public against dishonesty
12. Regulatory requirements relating to unlawful acts and dishonesty
13. Journalism in connection with unlawful acts and dishonesty
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
17. Counselling
18. Safeguarding of children and individuals at risk
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport
29. Consent
30. Vital interests
31. Not-for-profit bodies
32. Manifestly made public by the data subject
33. Legal claims
34. Judicial acts
35. Administration of accounts used in commission of indecency offences involving children
37. Insurance

Appropriate Policy Document

In many cases, for both Special Category Data and Criminal Offence Data there is a requirement to have an appropriate policy document in place to meet a UK Schedule 1 condition for processing in the DPA 2018.

APPENDIX C

Glossary

Consent – Permission by the data subject to process their personal data. The consent must be freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement, or by a clear affirmative action, signifies agreement to the processing of their personal data. Consent can be withdrawn at any time.

Data Controller – The person who (either jointly or in common with other persons) determines the purposes for and the means in which any personal data is or are to be processed.

Note: The Data Controller is usually a company or organisation and is not an individual within that company or organisation.

Data Subject – Any living individual who is the subject of personal data.

Personal Data – Any information relating to an identified or identifiable person. This includes information which can directly or indirectly identify the individual and can include name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental economic, cultural, or social identity of that natural person.

Processing – Any treatment of personal data: it includes collecting, recording, organising, structuring storing, altering, retrieving, using, disclosing, sharing, making available as well as restricting, erasing, and destroying.

Processor - A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

"Special category" personal data
The following special categories of personal data must be treated with extra care. These are:

Racial/ ethnic origin
Political opinions
Religious or philosophical beliefs

Trade Union membership
Genetic/ Biometric data processed to identify and individual
Health data
Sex life or sexual orientation

Criminal convictions and offences data must also be treated with extra care.

APPENDIX D

Relevant Legislation, Policies and Privacy Notices

Common Law Duty of Confidence

The Human Rights Act 1998

Computer Misuse Act 1990

The Freedom of Information Act 2000 (FOI Act)

The Regulation of Investigatory Powers Act 2000 (RIPA)

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)

The Environmental Information Regulations 2004 (SI 2004/3391)

The Criminal Justice and Immigration Act 2008

Data Protection Act 2018

UK General Data Protection Regulation

Information Risk Policy

Data Quality Policy

This list is not exhaustive

APPENDIX E

Data Protection Impact Assessments

Introduction

Under the new GDPR legislation, there is an obligation for organisations, in their role as data controllers, to conduct a data protection impact assessment ("**DPIA**") before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purpose.

Article 35 of GDPR introduces the formal requirement for a DPIA and it can best be described as a type of risk assessment which is carried out prior to a new processing activity, to highlight the viability of carrying out such a process and identifying any risks that may be associated with the processing.

When is a DPIA required?

Article 35 sets out the circumstances where a DPIA is required and states:

"*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact** of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

Although GDPR does not specifically state what must be covered by a DPIA, Article 35(7) sets out the following minimum requirements that should be considered:

- A systematic description of the proposed processing operations
- The purposes of the processing
- The legitimate interest pursued by the controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks, including appropriate:
    - Safeguards;
    - Security measures; and
    - Mechanisms to ensure the protection of personal data and to demonstrate compliance considering the rights and legitimate interests of data subjects and other persons concerned.

When is a DPIA not required?

The GDPR doesn't specifically state when a DPIA is not required, but there is significant guidance which can be relied upon when deciding whether a DPIA is required or not. From this guidance several circumstances have been identified where a DPIA is not required. These are:

- Where processing is low risk (i.e. not likely to result in a high risk to the rights and freedoms of natural persons).
- Where a DPIA has already been carried out and the nature, scope, context, and purposes of the processing are very similar to the proposed processing.
- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis.
- Where the processing is included on the optional list (established by the ICO) of processing operations for which no DPIA is required

A useful resource to DPIAs can be found at the ICOs website (link provided below):

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

This briefing note is accompanied with a template DPIA which has guidance and screening questions to help you ascertain whether a DPIA is necessary or not. These screening questions are based on ICO guidance.

Action Plan

These are a few points that you should consider when looking at DPIAs and whether you feel it is necessary to carry out an assessment:

- Be aware of the data you / your department processes and regularly assess whether this is due to change. If your department has been tasked with a new exercise, go through the screening questions on the template DPIA to determine whether you need to carry out the assessment.
- Look for any potential risk factors associated with the data you process and determine whether an assessment is needed.

Document Information and Version Control

Document name	Data Protection Policy
Document description	Data Protection Policy
Document status	Current
Lead officer	Alexa Baker, DPO
Sponsor	Lorraine Gore, SIRO
Produced by (service name)	Legal
Relevant to the services listed or all BCKL&WN	All BCKL&WN
Approved by	Cabinet / Full Council
Approved date	tbc
Type of document	Policy / Procedure
Equality Impact Assessment details	Not required
Review interval	Every 2 years or changes to legislation
Next review date	November 2025
Implementation and distribution	Policy will be published on InSite and publicised via internal Staff Update.
Retention	Information relating to FOI and DP requests/responses will be retained in line with the council's retention schedule.

•

Version	Originator	Description / reason for change	Date
0.01	Cara Jordan	Introduction of GDPR	May 2018
0.02	Lee Osler	Review period / following UK GDPR	Nov 2022
0.03	Laura Botten	Review period	Nov 2023