# DATA PROTECTION POLICY

# 1. Document Information

| | |
|---|---|
| **Title:** | **Data Protection Policy** |
| **Status:** | **FINAL** |
| **Current Version:** | **2.1** |
| **Author/s:** | **Vanda Niemiec – Senior Information Management Officer and Deputy Data Protection Officer**<br>Vanda.niemiec@iow.gov.uk<br>☎ (01983) 821000 Ext 6329 |
| **Sponsor:** | **Justin Thorne – Strategic Manager of Legal Services & Deputy Monitoring Officer**<br>Justin.thorne@iow.gov.uk<br>☎ (01983) 821000 Ext 6334 |
| **Consultation:** | ICT; CIU; IGG |
| **Approved by:** | **Christopher Potter – Data Protection Officer** |
| **Approval Date:** | October 2022 |
| **Review Frequency:** | Every 2 years |
| **Next Review** | October 2024 |

| Version History | | |
|---|---|---|
| **Version** | **Date** | **Description** |
| 1.0 | June 2018 | New policy for GDPR and Data Protection Act 2018 |
| 1.1 | Sept 2018 | Approved Policy for publication |
| 1.2 | Sept 2019 | Addition of missing Appendix 1 content |
| 1.3 | Oct 2019 | Policy update to reflect change of wordage associated with the Data Protection Officer contact |
| 1.4 | Dec 2019 | Format Update |
| 2.0 | Dec 2019 | Approved Policy for publication |
| 2.1 | June 2022 | Policy review post-Brexit and introduction of UK GDPR |

# 2. Contents

## 3. Introduction

The General Data Protection Regulation and Data Protection Act 2018 replaced the Data Protection Act 1998 in May 2018. Following the decision of the UK to leave the European Union, the UK Data Protection Regulation came into effect on 1 January 2021. It is now this legislation which governs how personal data should be handled to protect individuals in the UK (with the DPA 2018 and the UK GDPR hereinafter collectively referred to as data protection legislation).

The Council is classed as a Data Controller under data protection legislation as it collects, stores and controls how personal information is managed.

Consequently, it is required to hold, manage and process any personal data fairly, lawfully and in accordance with all data protection legislation requirements.

## 4. Scope & Purpose

The purpose of this policy is to define the Council's responsibilities under data protection legislation, providing assurance that all personal data is managed in compliance with statutory obligations.

This policy applies to all who have access to personal data held by the council, whether employees, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers. It includes those who work at home or have remote or flexible patterns of working.

## 5. Policy Statement

This policy sits within the Information Governance Framework which includes policies on Information Security and Freedom of Information.

This policy will be reviewed every 2 years as part of the information governance assurance program.

## 6. Confidentiality and Security

The council recognises the importance of the personal information it processes.

Personal data should be managed carefully and processed in accordance with the data protection legislation. The council also recognises that Article 8 of the Human Rights Act 1998 affords protection to individual's personal information. This means that the council will only seek to process personal information that may infringe this right where it is lawful, proportionate and necessary to do so.

Some personal data may also attract a duty of confidence initially, particularly when given in a health or social work environment.

Employees, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers have a duty to ensure that personal information is not knowingly or recklessly misused, lost, or destroyed.

- Manual files (paper records) - access must be restricted solely to relevant staff and stored in secure locations (eg lockable cabinets), to prevent unauthorised access.
- Computer systems will be configured, and computer files created, with adequate security levels to preserve confidentiality, and ensure only those that need access have access. Those who use the council's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work. Access will only be provided once relevant training has been undertaken and appropriate authorisation given.
- Those with access to personal information must comply with all council policies relating to the management of information including: use of electronic equipment and email, information security, protective markings. All policies are available on the council's intranet and internet sites, as appropriate.
- Personal data will be disclosed only to the data subject (the individual the information relates to) and those who are entitled to have access to it for the provision of a service or for a legal obligation. The Privacy notice that is issued at the time of collecting personal data will explain who the data may be shared with.
- At certain times it may be required that personal data be disclosed under one of the exemptions within the data protection legislation. These exemptions allow for personal data to be shared for the purposes of the prevention or detection of crime; or the assessment or collection of tax, for example, without gaining consent from the data subject. If there is a requirement for this, appropriate authorisation will be obtained, and an audit trail will be kept to provide accurate records of any disclosures of personal data.
- The council will ensure that appropriate technical and organisational measures are taken when transferring personal information, in accordance with our security policy. The level of security will be proportionate to the damage that may arise in the event of a security breach or loss of data. Sensitive personal data, whether being sent electronically or on paper, should only be transferred via a secure means as detailed in our Protective Marking Policy.

## 7. Obligations on staff and elected members

All individuals who have access to personal information at work have a personal responsibility to ensure that all processing complies with data protection principles. All employees are required to undertake training on data protection to ensure they are aware of their responsibilities for handling personal data.

Personal data should not be shared without being satisfied that the other party has a right to have the data. This may include obtaining appropriate authorisation or checking the relevant contract/Data Exchange Agreement/Information Sharing Protocol. These agreements/protocols govern what information will be shared, with which organisations and under what circumstances. They should include practical arrangements for how we and our partners will manage information in accordance with the data protection legislation and related policies.

Any individual who knowingly, or recklessly, processes data for purposes other than those for which it is intended, or is deliberately acting outside of their recognised responsibilities, may be subject to the council's disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution. All individuals permitted to access personal data in line with their work duties must comply with this policy and agree to undertake any relevant training that may be appropriate to the job/position they are working in.

As well as the council, individuals can also be prosecuted for unlawful action under the act. Upon summary conviction (in a Magistrate's Court), fines of up to £5000 could result if employees process information about other people without their consent or proper authorisation from the council. Upon conviction or indictment (Crown Court), the fine can be unlimited. Employees could be committing an offence by sharing information with others who do not need to be told that information in order to carry out their legitimate council duties.

Any complaint that alleges that the council, or a member of staff, has failed to comply with data protection legislation, should be sent to the Corporate Information Unit ("CIU") who will investigate on behalf of our Data Protection Officer and Caldicott Guardian. In addition, any incidents relating to the loss of; inappropriate access to; unlawful sharing of, personal data, must also be reported to the CIU (email: ciu@iow.gov.uk).
The Isle of Wight Council's Data Protection Officer is based at County Hall, Newport, Isle of Wight, PO30 1UD. (email: dpo@iow.gov.uk)

## 8. Definitions

a) **Personal Data –** data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

b) **Special Categories of Personal Data or Sensitive Personal Data –** data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, or criminal activity.

c) **Processing Personal Data –** is essentially any action involving personal data, this can include storing, sharing, creating, altering, organising or deleting. It is not limited to these examples and applies to both physical and electronically held data.

d) **Data Subject –** is an individual who is the subject of personal data.

e) **Data Controller –** is a person or organisation who decides the purposes for processing personal data. The Isle of Wight Council is a data controller.

f) **Data Protection Officer** (DPO) – is the designated person within an organisation that has responsibility for ensuring ‘legal’ compliance with GDPR, which relates only to personal data. The DPO for the Isle of Wight Council can be contacted at dpo@iow.gov.uk.

## 9. Categories of Individuals

The Council is a unitary authority and provides a number of services including Social Services for Adults, Children and Families; Housing; Planning; Council Tax; Housing Benefit; Environmental Health; Licensing; Leisure; and Parking Services. Therefore, the Council will process a significant amount of personal data relating to all individuals who may engage with these service areas. The information processed may include special categories of personal data as detailed above.

## 10. Overseas Data Transfer

Personal data shall not be transferred to a country outside the European Union 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.

## 11. Obtaining, Recording, Using and Disclosing

- **Processing**

Each of these activities comes within the definition of processing. Processing in relation to personal data, means carrying out any of the processing activities "on the data".

Any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data.

This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. (It is difficult to envisage any activity, which does not amount to processing)

All processing of personal data will comply with the data protection principles. In the situation where a third-party processes data, the third party will be required to act in a manner which ensures compliance with data protection legislation and have adequate safeguards in place to protect the personal data.

- **Obtaining**

  It is a requirement that any data collection forms used in order to collect personal data will contain a "Privacy Notice". The statement will need to be clearly visible and placed appropriately so the data subject (individual to whom the information relates) is fully aware of the intended uses of their personal data. It should also include as a matter of good practice, the padlock symbol to assist drawing to the attention that personal information is being collected.

  The information that would need to be supplied on a fair processing notice is as follows:

  - The identity of the data controller or appointed representative
  - The purpose or purposes for which the information is intended to be processed
  - Any further information in order to make the processing fair.
  - Who the data will be shared with
  - How long it will be retained
  - Details of the data subjects' rights

  It is also very important to remember, that when collecting data via the telephone or face to face, the above information should also be made clear to the data subject before any processing of their personal data takes place.

  The council will carefully consider the purposes for which it will use the personal information collected, both at the instant of collection and in the future. Before any further use of the information is considered the council will check the original fair processing notice given. If it is an unrelated purpose, that is not exempted by legislation such as for the purposes of crime prevention, then the council may not be authorised to use the information.

- **Recording and using the data**

  Data will only be processed for the purpose for which it was collected and should not be used for additional purposes unless permitted by legislation.

  At the time of collection, the council will inform all individuals of why their personal data is being collected. This will include the inclusion of a privacy notice on all forms, explaining what information is needed and why; who it will be shared with; how long it will be retained for etc. All information will be processed fairly and lawfully and in line with the purpose for which it has been given. In most cases, the council will need to hold and process information in order to carry out statutory obligations.

- **Disclosing**

  Personal data must not be disclosed, except to authorised users, other organisations and people who are pre-defined as a notified recipient, or if required under one of the exemptions within the data protection legislation.

The Corporate Information Unit (CIU), Legal Services, co-ordinates requests for personal information from other agencies such as the police, other local authorities and partner agencies. This is to ensure that there is a justified reason to share, and to apply consistency and for audit purposes. CIU will then contact the relevant department/s to discuss the request.

## 12. The Six Principles of GDPR

Data protection legislation sets out statutory principles that form the basis of the council's main responsibilities under the legislation. One such principle is the accountability principle which requires organisations to be able to demonstrate how they comply with the other following principles.

| Principles |
|---|
| 1. Processed lawfully, fairly and in a transparent manner in relation to individuals. |
| 2. Collected for specific, 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 historic research purposes or statistical purposes shall not be considered incompatible with the initial purpose. |
| 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it permits identification of data subjects for no longer than is necessary for the purposes for which the personal processed. |
| 4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay |
| 5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the GDPR in order to safeguard the rights and freedoms of individuals. |
| 6. 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. |

The Council is able to demonstrate it meets the above principles by way of the following policy aims.

## 12.1 Lawfulness of processing conditions

Under Data Protection legislation, the council needs to identify a lawful basis on which they can process an individual's data. These are referred to as the "conditions for processing" or legitimising reasons.

The Council is required to ensure it meets the conditions for processing and will need to explain to individuals whose data it holds, how it meets those conditions and what the individuals' rights are to ensure their data is managed appropriately.

The table below sets out the lawful basis for processing personal data. When the council collects personal data, it will issue a Privacy Notice which will clearly explain what lawful basis is relevant for the specific data collection.

| Conditions for processing |
|---|
| 6 (1) (a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes; |
| 6 (1) (b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract |
| 6 (1) (c) Processing is necessary for compliance with a legal obligation to which the controller is subject |
| 6 (1) (d) Processing is necessary to protect the vital interests of a data subject or another natural person. |
| 6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. |
| 6 (1) (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (this shall not apply to processing carried out by public authorities in the performance of their tasks.) |

## 12.2 Special conditions for sensitive (special categories) personal data

In addition to the above conditions, where the Council processes special categories of personal data, it must also be also able to demonstrate that it satisfies one of the conditions below.

| Condition for processing special categories of data |
|---|
| 9 (2) (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject; |

| |
|---|
| 9 (2) (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 in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; |
| 9 (2) (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. |
| 9 (2) (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 and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; |
| 9 (2) (e) Processing relates to personal data manifestly made public by the data subject. |
| 9 (2) (f) Processing is necessary for the establishment, exercise or in defence of legal claims or where courts are acting in their judicial capacity. |
| 9 (2) (g) Processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject domestic law; |
| 9 (2) (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 and services on the basis of domestic law or pursuant to contract with a health professional |
| 9 (2) (i) Processing is necessary for the 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 healthcare and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy domestic law. |
| 9 (2) (j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. |

## 12.3 Individuals' Rights

One of the key obligations on organisations who manage and control individuals' data is to ensure the individual is informed about their rights under data protection legislation, which gives them control over how their information is used and by whom.

The data subject's rights may be qualified, which means that there may be occasions when we are unable to comply with the request due one of the exemptions specified in the act or regulations applying. If an exemption is applied, the council will notify the data subject of which exemption applies and give reasons for the decision to apply the exemption.

These rights are detailed as follows

**a) The right to be informed**

This is the right to know how information is used and who it will be shared with. The Council has a Privacy Notice on its website (www.iwight.com) which outlines how personal data is managed. In addition, whenever the council collects personal data, a Privacy Notice will be issued detailing what information is needed and why, who it will be shared with, how long it will be held for and details of the rights an individual has for access/rectification/erasure. The notice will also include details of the Data Protection Officer.

Should an individual feel that the information supplied in the Privacy Notice is inadequate or that it doesn't inform them about the how their information is used by the Council, please contact the Council's Data Protection Officer for more information at dpo@iow.gov.uk.

**b) The right of access**

This is an individual's right to obtain

- confirmation that data is being processed;
- access to personal data; and
- access to policies and information held by the council about how it uses data

This right enables individuals to verify that the Council is using data appropriately, as well as providing access to obtain copies of information it holds.

Individuals are entitled to see the information held and can request a copy by emailing information@iow.gov.uk. Requests should clearly identify which council department may hold the information or which department/s the individual has had contact with, to assist with identifying relevant information. There is also a form available to submit a request which may assist with clarifying what information is sought.

A reply will be sent within one month of the date of the request, providing copies of the information held. However, should a request be more complex, the Council may require additional time to deal with the matter, in which case the council will contact the requestor and inform them of the delay

**c) The right to rectification**

Individuals have a right to ask to have information amended or rectified if they believe it is inaccurate or incomplete.

If individuals believe any information we hold about them to be incorrect, they should contact the relevant department in the first instance. If not resolved they should escalate to CIU at infomation@iow.gov.uk.

We will deal with all requests and consider whether any amendment, or annotation, is necessary.

**d) The right to erasure/ right to be forgotten**

This right allows individuals to request an organisation to delete information they hold about them.

However, the right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent (where consent was relied upon for the processing).
- When the individual objects to the processing and there is no overriding public interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the data protection legislation).
- The personal data has to be erased in order to comply with a legal obligation.

Requests will be considered on a case-by-case basis, taking into account the purpose for the holding of the personal data. Where a service is still being provided, or where there are legal obligations to retain personal data, the request may be refused.

**e) The right to restrict processing**

Individuals have a right to limit how their personal data is used, including who it is shared with.

A request for information to be used for limited purposes will not delete the information the Council holds.

Should you wish the Council to limit how we use your data please email dpo@iow.gov.uk with the reasons for your request.

**f) The right to data portability**

This right enables individuals to obtain electronic copies of information that they have provided to the Council, in a format that is easily transferred to either individuals or another organisation. This right is limited to that data that has been provided by the data subject in an electronic format and is held by the council is an electronic format.

**g) The right to object**

In addition to the right to limit the use of data, individuals also have a right to object to the use of data for certain actions. If an organisation agrees to your objection, it must stop using your data for that purpose unless it can give strong and legitimate reasons to continue using your data despite your objections.

The Council will consider each case on an individual basis and will take appropriate steps to ensure requests are complied with but that it also fulfils any legal obligation it has to provide information or supply services.

**h) Children's data**

Data protection legislation provides greater rights and protection to children's data, as children may be less aware of the risks and consequences associated with the processing of their personal data.

Children aged 13 or above are generally regarded as having the appropriate level of understanding to provide their own consent for the use of their data, provided the Privacy Notice has been written in a way they can understand.

## 13. How to exercise your data subject rights

Where an individual data subject has a question or complaint regarding their rights they are encouraged to make contact in writing (email) to the Council's Corporate Information Unit (information@iow.gov.uk) in the first instance.

Data subjects who consider that data is inaccurate or out of date are asked to contact the Corporate Information Unit, providing details of what information should be corrected or erased. A response will be sent within one month, advising whether the request can be agreed and what action has been taken.

A notice may be served by the data subject objecting to the processing and/or way in which the information is being processed, requesting the Council to cease doing so on the basis that this may cause substantial unwarranted damage or distress to the data subject. A written response indicating the Council's intentions will be given within one month of receiving the request. This will explain whether or not the Council intends to comply with the request, including any parts of the request which the Council considers unjustified.

Data subjects may ask the Council for an explanation of any decision likely to significantly affect them which has been, or may be, taken solely by wholly automated means, The Council will consider a request and consider reviewing a decision which has been taken, or, consider taking a new decision on a different basis, in circumstances where either course of action is appropriate and timely, unless the automated decision qualifies as an exempt decision.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be referred to the Council's Data Protection Officer for internal review.

Ultimately if a data subject continues to be dissatisfied, they have the right to appeal to ask the Information Commissioner's Office (ICO).

## 14. Process for reasons of legal duty

The council may receive requests for disclosure or other processing of personal data from partner agencies. This can include processing that is required to comply with court orders, or requests from the police or other enforcement body for the purposes of crime prevention or prosecution.

## 15. Data processors and partner agencies

All partner agencies, contractors or other data processors that the council contracts with must demonstrate the technical and operational ability to uphold the principles of data protection legislation

The council will expect partner agencies that act on our behalf to enter into appropriate contractual clauses or data processing agreements to ensure that each party understands their respective responsibilities under the data protection legislation.

## 16. Data Protection Impact Assessments (DPIAs)

The Council will ensure that any new or altered processing identifies and assesses the impact on a data subject's privacy as a result of any processing of their personal data, and that appropriate Privacy Notices are maintained to inform data subjects of how their data will be used. These will be assessed in line with the Data Protection Impact Assessment attached at Appendix 1.

Data Protection Impact Assessments should be completed at the start of any new project that involves the processing of personal data. Under data protection legislation they are required (mandatory) for certain listed types of processing, or any other processing that is **likely to result in a high risk** to individuals' interests. This includes where you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.
- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach

The Council is adopting good practice and is recommending that these agreements are completed for all projects that involve the processing/sharing of personal data.

The purpose of a DPIA is to
  - describe the nature, scope, context and purposes of the processing;
  - assess necessity, proportionality and compliance measures;
  - identify and assess risks to individuals; and
  - identify any additional measures to mitigate those risks.

## 17. Data Sharing Agreements

The council will write, uphold and regularly review Data Sharing Agreements when sharing information with other parties. Data Sharing Agreements are to be used where there is routine sharing of personal data, both internally between council departments and externally with partner agencies and other third parties.

All contracts with third parties should include a data processing schedule that includes all data sharing details. Where these are in place, there is no need for a separate data sharing agreement.

Where there is no contract in place, a data sharing agreement should be completed to formalise the routine sharing of data, including details of what will be shared, for what purpose and the security and retention arrangements.

All of the Council's data sharing and data processing arrangements are written in line with the ICO's Data Sharing Code of Practice, ICO's guidance on the role of Data Controllers and Data Processors and relevant council policies. These agreements will be reviewed every 2 years, unless stipulated otherwise.

## 18. Data Protection Officer (DPO)

The Data Protection Officer is responsible for ensuring compliance with this policy and overall information governance across the Council.

The DPO is assisted with their responsibilities by appointed deputies and the Corporate Information Unit (a team of information governance specialists)

## 19. Training

All council staff must complete training on data protection on an annual basis. In addition to the corporate training, individual service areas will include relevant training dependent on the type of data processed. This will include system training which will include the security of data where personal data is processed.

## 20. Personal Data Breaches

The Council has a process in place to ensure all staff know when and how to report any actual or suspected data breach, and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

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.

If a personal data breach occurs, then the Council will consider whether this poses a risk to people. The council will consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. If after this assessment the Council considers there will be a risk, then the Council must notify the ICO; if it's unlikely then the Council will record the incident but not report it. If there remains uncertainty the council will seek the guidance of the ICO

Data Protection legislation imposes a duty on the Council to report data breaches to the Information commissioner's office within 72 hours of becoming aware of the breach. In some cases, it is also required to notify the data subjects where it is considered there may be a high risk to their privacy.

All employees, elected members, partner agencies, contractors, have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Data Breach Incident Reporting Form found on the intranet.

If relevant the investigating officer may refer the breach to the appropriate manager and or human resources so that they may investigate whether the breach may also require separate disciplinary proceedings.

Any incidents of data breach or near miss should be reported to the Corporate Information Unit on the form that is available on the intranet.

EXAMPLE - Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Further advice on any aspects of processing personal data is available from the Corporate Information Unit at ciu@iow.gov.uk.

# 21. Appendix 1

## Data Protection Impact Assessments (DPIAs)

### 1. Introduction

This document sets out the procedure that should be used for any new processes that involve the processing of personal data. This will ensure that they meet confidentiality and data protection requirements.

The General Data Protection Regulation (GDPR) introduces new responsibilities on organisations to demonstrate that appropriate measures have been taken to ensure personal data is processed appropriately. DPIAs will help support the accountability principle, to demonstrate compliance.

The completion of a DPIA will assist officers in clarifying what information is needed to facilitate the new project/process and consider the legal basis and security arrangements at the outset. The process will also help the council to identify, assess and mitigate or minimise privacy risks with data processing activities. They are particularly relevant when a new data processing process, system or technology is being introduced

Failure to adequately conduct a DPIA where appropriate is a breach of the GDPR and could lead to fines of up to 2% of an organisation's annual global turnover or €10 million – whichever is greater.

### 2. When should a DPIA be conducted?

The GDPR mandates a DPIA be conducted where data processing “is likely to result in a high risk to the rights and freedoms of natural persons”. The three primary conditions identified in the GDPR are:

- A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
- Systematic monitoring of a publicly accessible area on a large scale.

The GDPR does not define what constitutes large-scale, but the following factors, must be considered:
a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
b. the volume of data and/or the range of different data items being processed;
c. the duration, or permanence, of the data processing activity;
d. the geographical extent of the processing activity.

However, the completion of a DPIA is recommended whenever a new project/contract/process is being considered that involves the processing/sharing of personal data.

## 3. Questions to ask before conducting a DPIA

Some simple questions you should ask yourself before undertaking a PIA, that will help inform the completion of the assessment:

1. What are you collecting? – Personal identifiable data, special categories of data,
2. Why are you collecting? – what is the legal basis, performance of a contract, legal obligation, consent
3. How are you collecting? – from data subject, extraction, questionnaire
4. Who are you sharing with? –joint data controllers, third parties
5. Where is it stored? – paper or electronic, security
6. How is it accessed? – access control, audit trails, logs, etc
7. Who is responsible for it? – data controller, third party/ies
8. When and how will it be destroyed? – retention policy
9. How will it be transported? – security arrangements

## 4. Process

The DPIA should be completed by the lead officer at the outset of any new project and agreed with all parties. Once completed it should be forwarded to the Corporate Information Unit (ciu@iow.gov.uk) for review.

When a DPIA has been approved it is important that the details contained in the assessment are reflected in any contract/process. This is to ensure that all parties, both internal and external to the Council, are aware of and agree to, their responsibilities. Contracts may contain a data processing agreement that includes these details. Dependant on the nature of the project this agreement may form the basis of a Data Sharing Agreement, for all parties to sign up to, where appropriate.

Further advice and guidance may be obtained from the Corporate Information Unit.

## Work flow details

| | | | |
|---|---|---|---|
| Project Name | | Point of contact for this work (name, role, phone, email) | |

| | |
|---|---|
| Service / department area concerned | |
| Project summary You may find it helpful to refer or link to other documents, such as a project proposal. | |
| Brief description of overall activity<br><br>Explain broadly what you aim to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA. | |
| Stakeholder(s) / Organisation(s) involved Has this project/process | |

| | |
|---|---|
| got the approval from the Stakeholders/ departments /partner agencies? | |
| **Information** | |
| What personal information will be collected (e.g. name, date of birth, medical/health, unique identifier, criminal record etc) How much data will you be collecting and using? How often? How many individuals are affected? | |
| Why is the information being collected? | |
| How will the information be collected? Provide details | Verbal ☐ Paper ☐ Electronic form ☐ Electronic (automated) ☐ |
| How will the information be stored? | Paper ☐ Electronic ☐ Other ☐→ |
| Where will the information be stored (including backups and copies?) | |
| How will the data be quality checked? | |
| Who is officer / service / department/ responsible for the | |

| | |
|---|---|
| information? | |
| What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? | |
| **Sharing and access** | |
| What information will be shared? | |
| Who will the information be shared with? | |
| How will the information be transported/ transferred? | |
| Which officers / roles will have access? Are there any restrictions based on different roles? | |
| How will the information be accessed? | |
| How will access be monitored (audit, logs?) | |
| What security measures will be in place? | |
| What information sharing protocols | |

| | |
|---|---|
| and operational agreements will be in place? | |
| What is your lawful basis for processing? Does the processing actually achieve your purpose? | |
| Will reports be generated from this information? If yes, will the information be anonymised? | |
| **Retention** | |
| How long will the data be retained? Where will it be stored? | |
| How will you destroy the information? (e.g. shredding,) | |
| If the organisation/service ceases what will happen to the information? | |
| **Risks, issues and activities** | |
| Any known risks or issues associated with the information? | |
| Any other relevant factors that needs to be considered? | |

| **Comments from Information Governance** | |
|---|---|
| **Comment** | **Date/author** |
| | |

**DEFINITIONS**

| | |
|---|---|
| UK General Data Protection Regulation (GDPR) | The EUGDPR replaced the Data Protection Act 1998 in May 2018 and introduced new requirements for data controllers and data processors. The UK GDPR came into effect on 1 January 2021 following the UK's decision to leave the European Union and governs data protection in the UK. |
| Data Controller | The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. |
| Data Processor | A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. |
| Legal basis for processing | **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.<br>**(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.<br>**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).<br>**(d) Vital interests:** the processing is necessary to protect someone's life.<br>**(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.<br>**(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.) |
| Personal data | Data which relates to an identified or identifiable natural individual (the data subject). May include name, address, date of birth, unique identifier, description, etc |
| Sensitive Data | Data which is more private/sensitive, and requires additional protection. It includes data relating to criminal activity as well as data defined under the GDPR as Special Categories of Personal Data:<br><br>• race;<br>• ethnic origin;<br>• politics;<br>• religion;<br>• trade union membership;<br>• genetics;<br>• biometrics (where used for ID purposes);<br>• health;<br>• sex life; or<br>• sexual orientation |
| | |