Mae'r ddogfen hon ar gael yn Gymraeg hefyd

Data Protection Policy & Procedures

Version	V4 2021	**Other Corporate Documents which may be referred to:** • Information Security Policy • Consent Policy • IT Security Policy • Subject Access Request Policy • Data Subject Rights Statement • Confidentiality Policy • Privacy Notice Procedure • Video and Call Recording Policy • Information Retention Schedules • Data Incident and Breach Procedure • Data Protection Impact Assessment Policy • Working from home/ Agile Working Statement
Author	Derek O'Connor	
Originally Approved by:	SMT	
Original Approval Date:	April 2018	
Date of next review	April 2024	
Date of Review Approval:		
Source Location	Information Governance S:\ drive, (GDPR)	
Location published (include relevant web link etc)	http://intranet.corp.conwy.gov.uk/en/Main/Information-Governance-Unit/Information-Governance-Unit.aspx	
Impact Assessment Completed date:	N/A	

Summary

What is this policy about?

This policy outlines Conwy County Borough Council's management and protection of personal data, and the rules everyone must adhere to.

Who is this policy for?

The policy applies to all staff, contractors, agency workers and elected members.

How does Conwy County Borough Council check this Policy is followed?

All staff and elected members must complete a mandatory online module on information management to evidence that they understand data protection legislation. Data Protection is part of the contractual terms with contractors and agency workers.

Who can you contact if you have questions about this policy?

Dylan Berrie
Information Governance Manager
Phone: 01492 577215
E-mail: info-gov.unit@conwy.gov.uk

1 Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of council business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2 Definitions

Council business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Council business purposes include (but are not limited to) the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring Corporate and service policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of official sensitive information, security vetting, and checking.* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and reviews* - *Monitoring staff conduct, disciplinary matters* - *Communication with the public*
Personal data	Information relating to identifiable individuals, such as clients, customers, job applicants, current and former employees, current and former elected members, agency, contract and other staff, clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV. (This list is not exhaustive)*
Special categories	Special categories data includes an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. *Any use of special categories data should be strictly controlled in accordance with this policy. Special categories also includes biometrics, DNA, facial and fingerprint recognition.*
Data Controller and Data Processor	The data controller is the person (or business) who determines the purposes for which, and the way in which, personal data is processed. By contrast, a data processor is anyone who processes personal data on behalf of the data controller (excluding the data controller's own employees)

3 Scope

This policy applies to all staff, contractors, agency workers and elected members. **You must be familiar with this policy and comply with its terms.**

This policy supplements our other information governance policies which are all located on the intranet. These policies include:

- Information security policy
- IT security policy
- Internet acceptable use policy
- Email acceptable use policy
- Privacy Notices and Guidance
- Consent Policy
- Data Incident Policy
- Subject Access Request Policy

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be approved by Senior Management Team and circulated to staff.

4 Who is responsible for this policy?

The protection of data is everybody's responsibility. Accountability for compliance with Data Protection within the Council is the responsibility of the Senior Information Risk Owner (SIRO). The Data Protection Officer (DPO) has overall responsibility for the day-to-day implementation and review of this policy.

4.1 The Senior Information Risk Owner's responsibilities (SIRO)

- Establish an effective Information Governance Framework for the authority
- Act as the executive level champion for information within the authority
- Ensure information assets and risks within the authority are managed
- Promote compliance with statutory, regulatory and organisational information policies
- Establish a reporting and learning culture to allow the organisation to establish where problems exist and to develop strategies to prevent future problems occurring.

4.2 The Data Protection Officer's responsibilities: (DPO)

- Keeping the SIRO & Information Governance Group updated about data protection, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Co-ordinating responses to individuals who wish to know which data is being held about them.
- Checking and approving with third parties that handle the authority's data, any contracts or agreement regarding data processing.

4.3 Designated Service Data Protection Lead

- Acting at the key service link between the DPO and the service
- Regular review and upkeep of the service information asset register
- Processing and co-ordination data protection policies
- Processing data subject requests and freedom of information (FOI) requests.

4.4 Responsibilities of the Head of IT & Digital Transformation

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the authority is considering using to store or process data

5 Principles

The data protection legislation & principles set out the main responsibilities for organisations.

Personal data shall be:

1) processed lawfully, fairly and in a transparent manner in relation to individuals;

2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) 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;

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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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 ability to ***demonstrate*** compliance is a key change which everyone processing personal data must comply.

6 Procedures

6.1 Privacy Notices - transparency of data protection

Data protection legislation states that we must have privacy notices which are *specific* to activity which requires personal information.

The privacy notice:

- Sets out the purposes for which we hold personal data
- Highlights that our work may require us to give information to third parties
- Provides that citizens have a right of access to the personal data that we hold about them

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following questions must be answered when processing personal data:

What information is being collected?
Who is collecting it?
How is it collected?
Why is it being collected?
How will it be used?
Who will it be shared with?
List the identity and contact details of any data controllers
List the details of transfers outside of European Economic Area (EEA) and safeguards
What is the retention period?

Please refer to Privacy Notice templates and procedure.

6.2 Personal Data

We must process personal data fairly and lawfully in accordance with individuals' rights.

The lawful basis for processing personal data requires that at least one of the following conditions **must** apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply to public authorities processing data to perform official tasks.

6.3 Special Categories data

Special category data is personal data which is more sensitive, and so needs more protection.
In order to lawfully process special category data, you must identify both a lawful basis for processing personal data (see para 6.2) and a separate condition for processing special category data as outlined below. These 2 conditions do not have to be linked.
There are currently ten conditions for processing special category data but additional conditions and safeguards may be added.
You must determine your condition for processing special category data before you begin this processing, and you should document it.

In most cases where we process special categories data we will require the data subject's consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The lawful basis for processing special categories data requires that in addition to the conditions listed in paragraph 6.2, you must also apply at least one of the following conditions whenever you process special categories data:

a) **Explicit consent of the data subject,** unless reliance on consent is prohibited by EU or Member State law.
b) Necessary for the **carrying out of obligations** under employment, social security or social protection law, or a collective agreement.
c) Necessary **to protect the vital interests** of a data subject who is physically or legally incapable of giving consent – this is the equivalent of the wording in the DPA.
d) Processing carried out in the course of its **legitimate activities with appropriate safeguards** by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
e) **Data manifestly made public** by the data subject.
f) Necessary for the **establishment, exercise or defence of legal claims** or where courts are acting in their judicial capacity.
g) Necessary for reasons of **substantial public interest** on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures – this means that Member States can extend the circumstances where sensitive data can be processed in the public interest.
h) Necessary for the purposes of **preventative or occupational medicine,** for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
i) 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 healthcare and of medicinal products or medical devices
j) Necessary for **archiving purposes in the public interest, or scientific and historical research** purposes or statistical purposes.

7 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask us to correct inaccurate personal data relating to them.

We will make it clear to citizens that they must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required. This will be communicated through the Council's Privacy notice.

8 Data security

Staff, agency staff, contractors and elected members must protect personal data and keep it secure, to prevent loss or misuse. Where other organisations process personal data as a service on our behalf, services must liaise with the DPO to establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

9 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed and/or confidential waste?
- Data stored on a computer should be protected by strong passwords.
- Data stored on external devices must be encrypted and locked away securely when they are not being used
- Any cloud used to store data must have the prior approval of the Head of IT & Digital Transformation.
- Servers containing personal & special categories data must be kept in a secure location.
- Data should be regularly backed up in line with our backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All personal and special categories data stored on the company's IT systems must be identified using the Corporate Data Classification solution and handled in line with the IT Security Policy.

10 Data retention

We must retain personal & special categories data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our **Retention Schedule Guidance**.

11 Information Sharing

The Data Protection Act is not a barrier to sharing information but rather provides a framework to ensure that personal information about living persons is shared appropriately. **Staff should not hesitate to share personal information in order to prevent abuse or serious harm, in an emergency or in life-or-death situations**. If there are concerns relating to child or adult protection issues, then the relevant procedures should be followed.

The Wales Accord on the Sharing of Personal Information (WASPI) was developed as a practical approach to multi agency sharing for the public sector in Wales, which the Council signed up to in June 2011.

Information sharing is key to joined up service delivery. Decisions on whether to share information must be taken on a case-by-case basis which should then be supported by the production of either an Information Sharing Protocol (ISP) or a Data Disclosure Agreement (DDA).

Each ISP and/or DDA must have a clearly defined purpose for the sharing and must be seen and registered by the Information Governance Unit before being signed off at Head of Service level.

12 Transferring data internationally

There are restrictions on international transfers of personal & special categories data. You must not transfer personal & special categories data anywhere outside the UK without first consulting the Data Protection Officer.

13 Data Subject's Rights

Data Protection legislation provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

1 The right to be informed

Individuals have the right to know that information about them is being processed. This is done through a privacy notice. The information that must be supplied is determined by whether or not the authority obtained the personal data directly from individuals. The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

2 The right of access (subject access requests)

Individuals are entitled, subject to certain exemptions, to request access to information held about them.
If you receive a subject access request, you should refer that request immediately to the Designated Service Data Protection Lead.

We will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the designated service data protection lead about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

3 The right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the personal data in question has already been to third parties, we must inform those third parties of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate. We must respond within one month. This can be extended by two months where the request for rectification is complex. Where we are not taking action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the Information Commissioner Office.

4 The right to erasure (also known as the right to be forgotten)

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies. We must respond within one calendar month.

5 The right to restrict processing

We will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether the authority's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- We may need to review procedures to ensure we are able to determine where you may be required to restrict the processing of personal data.

If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
We must inform individuals when we decide to lift a restriction on processing.

6 The right to data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free. The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

7 The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

8 Rights in relation to automated decision making and profiling.

Data Protection legislation makes provisions for:

- automated individual decision-making (making a decision solely by automated means without any human involvement);and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The legislation applies to all automated individual decision-making and profiling. There are additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

You must identify whether any of your automated decision making has legal or similarly significant effects on them. If so, make sure that you:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

14 Protection of children and vulnerable people

Where information is passed to the Council concerning safeguarding, then the risk posed and the individual's right to privacy will have to be balanced against each other.

If information received by the Council relating to any person(s) who may come into contact in any way with children and/or vulnerable persons raises concerns as to the appropriateness of the person(s) having contact with children and/or vulnerable people and/or as to the future well-being of such children and/or vulnerable persons, **the Council will consider it a duty to share that information**. It may be shared with any appropriate individual, company group, committee, Police Force and other Council or agency if the balance of risk is deemed to require the sharing of such information.
CONWY COUNTY BOROUGH COUNCIL DEEMS THE DUTY TO SAFEGUARD VULNERABLE PEOPLE AS AN OVER-RIDING DUTY TO THE DUTY TO PROTECT INFORMATION.

15 Imagery

The Council will ensure, where necessary, that all the people who will appear in a photograph, video or web cam image are made aware that such recording is taking place, with the exception of CCTV where signage is used to alert the public in areas where cameras are covering public space. The Council will also make clear why it is using that person's image, what it will be used for.

Legal guidance states that by the age of 13 a child may be considered to have `sufficient maturity' to understand their rights under the Act.

However, The Council has decided that parental/ guardian consent should be sought up to the age of 18 years. However, the views of children aged 13 years and over should be considered.

16 Training

All staff and elected members will receive e learning training on data protection. New starters will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training can be access through the Corporate Training Programme

It will cover:

- The law relating to data protection
- Data protection and related policies and procedures.

Completion of training is mandatory.

17 Privacy by design and default

Privacy by design is an approach to projects, processes or activities that promote privacy and data protection compliance from the start. The service initiating a new project, process or activity will be responsible for conducting a Privacy Impact screening and if necessary a full assessment.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

18 International data transfers

No data may be transferred outside of the European Economic Area (EEA) without first discussing it with the data protection officer.

19 Information Asset Register and data audit

Each service will have a **data protection lead** who is responsible for the regular review and up keep of the service information asset register. Regular data audits to manage and mitigate risks will inform the data register. The asset register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

20 Reporting an incident

All members of staff & elected members have an obligation to report actual or potential data protection incidents **as soon as possible** to the DPO. This is necessary to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- If necessary, notify the Information Commissioner's Office (ICO) within 72 hours of any compliance failures that are material either in their own right or as part of a pattern of failures.

All staff should report any incidents or suspected incidents immediately via the Data Incident Report form (on self service area of intranet). **Please refer to our Data Incident Policy for our reporting procedure.**

PLEASE NOTE – *reporting an incident is not an automatic disciplinary*. It's a supportive approach to ensure we all act responsibly, support the member of staff, and deal with the situation quickly.

If an incident isn't reported when it should have been, this may have consequences not only for the authority but for the individual member of staff.

21 Consequences of failing to comply

Conwy County Borough Council takes compliance with this policy very seriously. Failure to comply puts both individuals and the authority at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our employment procedures which may result in dismissal. A failure in compliance may also lead to a fine being imposed upon the Authority.