LLANHARAN COMMUNITY COUNCIL
DATA PROTECTION POLICY

Purpose

The council is committed to being transparent about how it collects and uses the personal data of staff, and to meeting our data protection obligations. This policy sets out the council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the current Data Protection Act. The council understands that it will be accountable for the processing, management and retention of all personal data held.

This policy applies to the personal data of current and former job applicants, employees, workers, apprentices, volunteers, placement students and self-employed contractors, referred to as HR-related personal data.

The council has appointed the Clerk, Leigh Smith, as the person with responsibility for data protection compliance within the council. Questions about this policy, or requests for further information, should be directed to him.

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a ‘data subject’) on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

“Processing” is any use that is made of data, whether or not by automated means, such as collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

Data protection principles

The council processes HR-related personal data in accordance with the following data protection principles. The council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

In addition, personal data will be processed in recognition of an individual’s data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information

- the right to regulate any automated decision-making and profiling of personal data.

The council will tell you of the personal data it processes, the reasons for processing your personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

The council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it. The council will not process your personal data if it does not have a legal basis for processing.

The council keeps a record of ongoing (non-occasional) processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Processing

Personal data

The council will process your personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract
- it is necessary to comply with any legal obligation
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests
- it is necessary to protect the vital interests of a data subject or another person
- it 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.

If the council processes your personal data in line with the above, it does not require your consent. Otherwise, the council is required to gain consent to process your personal data. If the council asks for such consent, then we will explain the reason for the request. You do not have to consent and can withdraw consent later.

The council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.
Personal data gathered during the period of employment is held in your personnel file in electronic format on HR and IT systems and servers. The periods for which the

council holds your personal data are as follows:

Type of record	Retention period	Reason
Personnel	Six years after end of employment	Limitation period for civil claims
Disciplinary		
Payroll	Three years after end of relevant tax year	Compliance with HMRC regulations
Sick leave		
Health & Safety	Three years after incident	Compliance with HSE regulations
Health & Safety (hazardous substances)	Up to forty years after incident in certain circumstances	

Sometimes the council will share your personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

The council will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

Special categories of data

The council will only process special categories of your personal data (see above) in accordance with legislation where it is necessary:

- for carrying out rights and obligations under employment law or a collective agreement;
- to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- for the establishment, exercise or defence of legal claims;

- for the purposes of occupational medicine or for the assessment of your working capacity;
- for reasons for substantial public interest based on law which is proportionate to the aim pursued and which contains appropriate safeguards;
- for reasons of public interest around public health; and
- for archiving purposes in the public interest or scientific and historical research purposes;
- or where you have made the data public.

If the council processes special categories of your personal data in line with the above, it does not require your consent. In other cases, the council is required to gain consent to process your special categories of personal data. If the council asks for your consent to process a special category of personal data, then we will explain the reason for the request. You do not have to consent or can withdraw consent later.

Individual rights

As a data subject, you have a number of rights in relation to your personal data.

Subject access requests

You have the right to make a subject access request. If you make a subject access request, the council will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if not collected from yourself;
- to whom your data is or may be disclosed;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the council has failed to comply with your data protection rights; and
- Whether or not the council carries out automated decision-making and the logic involved in any such decision-making.

The council will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically unless you agree otherwise.

If you want additional copies, the council may charge a fee, which will be based on the administrative cost to the council of providing the additional copies.

To make a subject access request, send it to the Clerk or Chair of the Council. In some cases, the council may need to ask for proof of identification before the request can be processed. The council will tell you if we need to verify your identity and the documents we need.

The council will normally respond to a request within a period of one month from the date it is received. Where the council processes substantial amounts of your data, this may not be possible within one month. The council will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the council is not obliged to comply with it. Alternatively, the council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the council has already responded. If you submit a request that is unfounded or excessive, the council will notify you that this is the case and whether we will respond to it.

Other rights

You have other rights in relation to your personal data. You can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the council's legitimate grounds for processing data (where the council relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful;
- stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override the council's legitimate grounds for processing data.
- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask the council to take any of these steps, you should send the request to the Clerk or Chair of the Council.

Data security

The council takes the security of HR-related personal data seriously. The council adopts procedures designed to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

Some of the processing that the council carries out may result in risks to privacy (such as monitoring of public areas via CCTV). Where processing would result in a substantial risk to your rights and freedoms, the council will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for yourself and the measures that can be put in place to mitigate those risks.

Data breaches

The council has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, the council must take notes and keep evidence.

If you are aware of a data breach, you must contact the Clerk or Chair of the Council immediately and keep any evidence you have in relation to the breach.

If the council discovers that there has been a breach of HR-related personal data that poses a risk to your rights and freedoms, we will report it to the Information Commissioner within 72 hours of discovery. The council will record all data breaches regardless of their effect.

If the breach is likely to result in a substantial risk to the rights and freedoms of individuals, we will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures we have

taken.

International data transfers

The council will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities

You are responsible for helping the council keep your personal data up to date. You must inform the council immediately if you believe that the data is inaccurate, either because of a subject access request or otherwise. The council will take immediate steps to correct the information. You should let the council know if data provided to the council changes, for example if you move to a new house or change your bank details.

Everyone who works for, or on behalf of, the council has responsibility for ensuring data is collected, stored and handled appropriately, in line with the council's policies.

You may have access to the personal data of other individuals and members of the public in the course of your work with the council. Where this is the case, the council relies on you to help meet our data protection obligations to staff and members of the public. Individuals who have access to personal data are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

- Never to transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council
- to ask for help from the council's data protection lead if unsure about data protection, or if you notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may be dealt with under the council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

This is a non-contractual policy which will be reviewed from time to time.
Failure or refusal to sign an acknowledgement does not affect the application of this policy, which will apply to all employees from the date of issue.