LLANGORS COMMUNITY COUNCIL

GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018

Policies included in this file are held separately, but amalgamated into one file for ease of display on the website.

LLANGORS COMMUNITY COUNCIL

INFORMATION AND DATA PROTECTION POLICY

Introduction

All Councillors and staff of Llangors Community Council aim to ensure that the procedure it adopts regarding the handling and security of information complies with the highest ethical standards. It fully endorses the Data Protection Act 1998 and aims to adhere to the six principles of the General Data Protection Regulations (GDPR) 2018: - Personal data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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.

Data Protection Terminology

Data subject - means the person whose personal data is being processed.
That may be an employee, prospective employee, associate or prospective associate of the CC or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

Llangors Community Council is the Data Controller. The Clerk is the designated Data Protection Officer.

In order to conduct its business, services and duties, the Community Council processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

• Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.

• Confidential information and data not yet in the public arena such as ideas or policies that are being worked on.

• Confidential information about other organisations because of commercial sensitivity.

• Personal data concerning its current, past and potential employees, Councillors, and volunteers.

• Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

The Community Council will periodically review and revise this policy in light of comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Council's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information. The Community Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The Community Council processes **personal data** in order to:

• fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.

• pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.

• monitor its activities including the equality and diversity of its activities

• fulfil its duties in operating the business premises including security

• assist regulatory and law enforcement agencies

• process information including the recording and updating details about its Councillors, employees, partners and volunteers.

• process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.

• undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.

• undertake research, audit and quality improvement work to fulfil its objects and purposes.

• fulfil its duties as a burial board

• carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

• The individual has consented to the processing

• Processing is necessary for the performance of a contract or agreement with the individual

• Processing is required under a legal obligation
• Processing is necessary to protect the vital interests of the individual
• Processing is necessary to carry out public functions
• Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any **sensitive personal information** and the Community Council will ensure that at least one of the following conditions is met:
• Explicit consent of the individual
• Required by law to process the data for employment purposes
• A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?
The Community Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated the day to day responsibility to the Clerk as Data Protection Officer who can be contacted by email: clerk@llangors.org.uk

The Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.
Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Personal data shall not be transferred to a country or territory outside the European Economic Areas 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.

Information provided to us
The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with the Community Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however where ever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Council is able to keep their personal data accurate and up-to-date. The personal information will not be shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Councils Right to Process Information
General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e)
Processing is with consent of the data subject, or
Processing is necessary for compliance with a legal obligation.
Processing is necessary for the legitimate interests of the Council.

Information Security
The Community Council seeks to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies.
We will only keep your data for the purpose it was collected for and only for as long as is necessary, after which it will be deleted.

Children
We will not process any data relating to a child (under 16) without the express parental/ guardian consent of the child concerned.

Rights of a Data Subject
Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting the Data Protection Officer.

Information Correction: If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate.

Information Deletion: If the individual wishes the Council to delete the information about them, they can do so by contacting the Data Protection Officer.

Right to Object: If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Data Protection Officer.
The Council does not use automated decision making or profiling of individual personal data.

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Data Protection Officer or the Information Commissioners Office **casework@ico.org.uk** Tel: 0303 123 1113.
The Council will always give guidance on personnel data to employees.
The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

DATA & IT SECURITY POLICY

The Data Protection Act says security should be appropriate to:
• the nature of the information in question; and
• the harm that might result from its improper use, or from its accidental loss or destruction.

The Act does not define “appropriate”. It does say that an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved. The Act does not require an organisation to have state-of-the-art security technology to protect the personal data it holds, but a review of your security arrangements should regularly occur as technology advances. There is no “one size fits all” solution to information security, and the level of security chosen should depend on the risks to the organisation.

Computer security:
• Firewall and virus-checking installed on computer.

• Operating system set up to receive automatic updates.

• Download the latest patches or security updates, which should cover vulnerabilities to computer automatically

• Only allow Members access to the information they need to carry out their work and do not share passwords.

• Regular back-ups of the information on your computer system taken and kept in a separate place.

• All personal information will be removed before disposing of old computers (by using technology or destroying the hard disk).

• Anti-spyware tool installed. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Using emails securely:

• Before sending consider whether the content of the email should be encrypted or password protected.

• Take care when typing in the name of the recipient; some email software will suggest similar addresses that have been used before. If you have previously emailed several people whose name or address starts the same way - e.g. "Colin" - the auto-complete function may bring up several "Colin's". Make sure to choose the right address before clicking send.

• To send an email to a recipient without revealing their address to other recipients, make sure blind carbon copy (bcc) is used, not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

• Take care when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

• To send a sensitive email from a secure server to an insecure recipient, security will be threatened. Check that the recipient's arrangements are secure enough before sending your message.

For other security:

- Confidential paper waste will be shredded/burnt
- Physical security of premises considered

Training of staff:

• to know what is expected of them;

• to be wary of people who may try to trick them into giving out personal details;

• to use a strong password

• to not send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;

• not to believe emails that appear to come from the bank that ask for account, credit card details or password (a bank would never ask for this information in this way);

• to not open spam – not even to unsubscribe or ask for no more mailings. Delete the email and use spam filters on the computer.

An impact assessment/review will be carried out annually to ensure compliancy with GDPR and relevant policies of the Community Council.

Reviewed and Approved at the meeting of Llangors Community Council on ……

Signed by Chairperson……

LLANGORS COMMUNITY COUNCIL

GENERAL PRIVACY NOTICE – MEMBERS OF THE PUBLIC

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Llangors Community Council which is the data controller for your data.

Other data controllers the council works with:

- Local Authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Law enforcement agencies

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council property, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of

injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);

- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request, we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) The right to object to processing of your personal data or to restrict it to certain purposes only

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) The right to lodge a complaint with the Information Commissioner's Office.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this website www.llangors.org.uk. This Notice was last updated in July 2022.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Llangors Community Council

Email: clerk@llangors.org.uk

Reviewed and Approved at the meeting of Llangors Community Council on ……

Signed by Chairperson……

LLANGORS COMMUNITY COUNCIL

PRIVACY NOTICE

FOR STAFF*, COUNCILLORS AND ROLE HOLDERS**

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis

**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Llangors Community Council which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.

- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

- We may process sensitive personal data relating to staff, councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

- in order to comply with legal requirements and obligations to third parties.

- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. The right to object to processing of your personal data or to restrict it to certain purposes only

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. The right to lodge a complaint with the Information Commissioner's Office.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of

personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will notify you of any updates by email. This Notice was last updated in July 2022.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Llangors Community Council

Email: clerk@llangors.org.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Reviewed and Approved at the meeting of Llangors Community Council on ……

Signed by Chairperson……

LLANGORS COMMUNITY COUNCIL

WEBSITE PRIVACY POLICY

Llangors Community Council are committed to safeguarding the privacy of our website visitors; this policy sets out how we will treat your personal information.
Our website uses cookies. By using our website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy.

1. What information do we collect?

We may collect, store and use the following kinds of personal information:

1. information about your computer and about your visits to and use of this website (including your IP address, browser type and version, operating system, referral source, length of visit, page views and website navigation);
2. any other information that you choose to send to us;

2. Cookies

A cookie consists of a piece of text sent by a web server to a web browser and stored by the browser. The information is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.
We use "session" cookies on the website. We will use the session cookies to: keep track of you whilst you navigate the website; and remember your website preferences between page requests.
Session cookies will be deleted from your computer when you close your browser. Persistent cookies will remain stored on your computer until deleted, or until they reach a specified expiry date.
We use Google Analytics to analyse the use of this website. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to our website is used to create reports about the use of the website. Google will store this information. Google's privacy policy is available at: **http://www.google.com/privacypolicy.html**.
Most browsers allow you to reject all cookies, whilst some browsers allow you to reject just third party cookies. For example, in Internet Explorer you can refuse all cookies by clicking "Tools", "Internet Options", "Privacy", and selecting "Block all cookies" using the sliding selector. Blocking all cookies will, however, have a negative impact upon the usability of many websites, including this one.

3. Using your personal information

Personal information submitted to us via this website will be used for the purposes specified in this privacy policy or in relevant parts of the website.
We may use your personal information to:

1. enable your use of the services available on the website;
2. deal with enquiries and complaints made by or about you relating to the website;

4. Disclosures

We may disclose information about you to any of our employees, officers, agents, suppliers or subcontractors insofar as reasonably necessary for the purposes as set out in this privacy policy.
In addition, we may disclose your personal information:

1. to the extent that we are required to do so by law;
2. in connection with any legal proceedings or prospective legal proceedings;
3. in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);

4. to the purchaser (or prospective purchaser) of any business or asset that we are (or are contemplating) selling;
5. to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.

Except as provided in this privacy policy, we will not provide your information to third parties.

5. International data transfers

Information that we collect may be stored and processed in and transferred between any of the countries in which we operate in order to enable us to use the information in accordance with this privacy policy.

Information which you provide may be transferred to countries which do not have data protection laws equivalent to those in force in the European Economic Area.

6. Security of your personal information

We will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

We will store all the personal information you provide on our secure (password and firewall protected) servers.

Of course, data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

7. Policy amendments

We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes.

We may also notify you of changes to our privacy policy by email.

8. Your rights

You may instruct us to provide you with any personal information we hold about you. Provision of such information will be subject to:

1. no payment of a fee unless the request is manifestly unfounded or excessive;
2. the supply of appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address).

We may withhold such personal information to the extent permitted by law.

You may instruct us not to process your personal information for marketing purposes, by using the contact details below. In practice, you will usually either expressly agree in advance to our use of your personal information for marketing purposes, or we will provide you with an opportunity to opt-out of the use of your personal information for marketing purposes.

9. Third party websites

The website contains links to other websites. We are not responsible for the privacy policies or practices of third party websites.

10.Updating information

Please let us know if the personal information which we hold about you needs to be corrected or updated.

11. Contact

If you have any questions about this privacy policy or our treatment of your personal information, please write to us by email to clerk@llangors.org.uk

12. Data controller

The data controller responsible in respect of the information collected on this website is Llangors Community Council.

Reviewed and Approved at the meeting of Llangors Community Council on ……

Signed by Chairperson……

LLANGORS COMMUNITY COUNCIL

EMAIL CONTACT PRIVACY NOTICE

When you contact us
The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored to enable us to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

The Councils Right to Process Information
General Data Protection Regulations Article 6 (1) (a) (b) and (e)
Processing is with consent of the data subject or
Processing is necessary for compliance with a legal obligation or
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

Information Security
Llangors Community Council has a duty to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. Copies of these policies can be requested.
We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted.

Children
We will not process any data relating to a child (under 16) without the express parental/ guardian consent of the child concerned.

Access to Information
You have the right to request access to the information we have on you. You can do this by contacting the Clerk to the Community Council, clerk@llangors.org.uk

Information Correction
If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact the Clerk at clerk@llangors.org.uk

Information Deletion
If you wish Llangors Community Council to delete the information about you please contact the Clerk to request this.

Right to Object
If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact the Clerk to object.

Rights Related to Automated Decision Making and Profiling
Llangors Community Council does not use any form of automated decision making or the profiling of individual personal data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Llangors Community Council General Data Protection Officer, email clerk @llangors.org.uk. If you are unsatisfied with the response, you may contact the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Summary: In accordance with the law, Llangors Community Council only collects a limited amount of information about you that is necessary for correspondence, information and service provision. Llangors Community Council does not use profiling, we do not sell or pass your data to third parties. We do not use your data for purposes other than those specified. Llangors Community Council does its utmost to ensure your data is stored securely. We delete all information deemed to be no longer necessary. The Community Council constantly reviews its Privacy Policies to keep it up to date in protecting your data. Copies of all policies are available on request.

Reviewed and Approved at the meeting of Llangors Community Council on ……

Signed by Chairperson……

LLANGORS COMMUNITY COUNCIL

DOCUMENT RETENTION AND DISPOSAL POLICY TO COMPLY WITH GDPR

1. Introduction

1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.
1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.
1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.
1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.
1.5 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

2. Scope and Objectives of the Policy

2.1 The aim of this document is to provide a working framework to determine which documents are:
• Retained – and for how long; or
• Disposed of – and if so by what method.
2.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:
• 'With compliments' slips
• Catalogues and trade journals
• Invitations not accepted
• Trivial electronic mail messages that are duplicated or not related to Council business.
• Requests for general local information
• Out of date information
2.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.
2.4 Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulations.

3. Roles and Responsibilities for Document Retention and Disposal

3.1 Councils are responsible for determining whether to retain or dispose of documents and should undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the General Data Protection Regulations.
3.2 Councils should ensure that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

4.1 Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments to which they work.

4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

• Facilitate an audit or examination of the business by anyone so authorised.

• Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.

• Verify individual consent to record, manage and record disposal of their personal data.

• Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

4.3 To facilitate this the following principles should be adopted:

• Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations

• Documents that are no longer required for operational purposes but need retaining should be placed in applicable filing cabinets.

4.4 The retention schedule attached – "Policy for Documents Retention and Disposal" provides guidance on the recommended minimum retention periods for specific classes of documents and records.

4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

5. Document Disposal Protocol

5.1 Documents should only be disposed of if reviewed in accordance with the following:

• Is retention required to fulfil statutory or other regulatory requirements?

• Is retention required to meet the operational needs of the service?

• Is retention required to evidence events in the case of dispute?

• Is retention required because the document or record is of historic interest or intrinsic value?

5.2 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.

5.3 Documents can be disposed of by any of the following methods:

• Non-confidential records: recycling bin for disposal.

• Confidential records or records giving personal information: shred documents.

• Deletion of computer records.

• Transmission of records to an external body such as the County Records Office.

5.4 The following principles should be followed when disposing of records:

• All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.

• the Freedom of Information Act or cause reputational damage.

• Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.

• Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.

• Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

5.5 Records should be maintained of appropriate disposals. These records should contain the following information:
• The name of the document destroyed.
• The date the document was destroyed.
• The method of disposal.

6. Data Protection Act 1998 – Obligation to Dispose of Certain Data
6.1 The Data Protection Act 1998 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:
Data that relates to a living individual who can be identified:
a) from the data, or b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.
It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.
6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met.
6.3 Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations namely:
• Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
• Personal data shall only be obtained for specific purposes and processed in a compatible manner.
• Personal data shall be adequate, relevant, but not excessive.
• Personal data shall be accurate and up to date.
• Personal data shall not be kept for longer than is necessary.
• Personal data shall be processed in accordance with the rights of the data subject.
• Personal data shall be kept secure.
6.4 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

7. Scanning of Documents
7.1 In general once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.
7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.
7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

8. Review of Document Retention
8.1 It is planned to review, update and where appropriate amend this document on a regular basis.

9. List of Documents
The full list of the Council's documents and the procedures for retention or disposal can be found attached "Policy for Documents Retention and Disposal" List. This is updated regularly in accordance with any changes to legal requirements.

Reviewed and Approved at the meeting of Llangors Community Council on ……

Signed by Chairperson……

LLANGORS COMMUNITY COUNCIL

GENERAL DATA PROTECTION CONSENT FORM

Your privacy is important to us and we would like to communicate with you about Llangors Community Council and its activities. To do so we need your consent. Please read and understand the General Privacy notice of Llangors Community Council then fill in your name and address and other contact information below and confirm your consent by signing and by ticking the boxes below.

		If you are aged 16 or under your parent or guardian should fill in their details below to confirm their consent
Name	……	……
Address	……..	……
	……	……
	……	……
Signature	……	……
Date	……	……

You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from the Data Protection Officer, email: clerk@llangors.org.uk

You can withdraw or change your consent at any time by contacting the council.

☐ We may contact you to keep you informed about what is going on in the Council's area or other local authority areas including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, or in printed or electronic form (including social media).

☐ We may contact you about groups and activities you may be interested in participating in.

☐ We may use your name and photo in our newsletters, bulletins or on our website, or our social media accounts.

Keeping in touch:

☐ Yes please, I would like to receive communications by email

☐ Yes please, I would like to receive communications by telephone

☐ Yes please, I would like to receive communications by mobile phone including text message

☐ Yes please, I would like to receive communications by social media (for example Facebook, Twitter, Instagram, WhatsApp)

☐ Yes please, I would like to receive communications by post