CYNGOR CYMUNED LLANTRISANT
LLANTRISANT COMMUNITY COUNCIL

Parish Office
Newbridge Road
Llantrisant
CF72 8EX

01443 223796
office@llantrisant-cc.gov.wales
Clerk: Mr G E Hopkins JP BA(Hons)

Swyddfa'r Plwyf
Heol Pontnewydd
Llantrisant
CF72 8EX

01443 223796
office@llantrisant-cc.gov.wales
Clerc: Mr G E Hopkins JP BA(Hons)

LLANTRISANT COMMUNITY COUNCIL

GENERAL DATA PROTECTION REGULATION POLICY

CONTENTS:

This suite of policies was adopted by Llantrisant Community Council at its meeting on 10th December 2024.

General Data Protection Regulation Policy

Llantrisant Community Council is fully committed to protecting both its own and its client's data, and the rights and freedoms of all individuals in relation to the processing of their personal data.

1 Introduction

Llantrisant Community Council ("The Council") is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of The Council employees in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an The Council Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller: The Council as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose The Council to complaints, regulatory action, fines and/or reputational damage.

The Council's management team is fully committed to ensuring continued and effective implementation of this policy and expects all The Council Employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction. This policy has been approved by the Members of the The Council at Full Council under Minute reference XX/XX/XX.

2 Scope

This policy has been designed to establish the standard for the Processing and protection of Personal Data by all The Council Employees.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals:

- In the context of the business activities of The Council; and,
- During the provision of the day to day running of the The Council.

The protection of Personal Data belonging to The Council Employee data is not within the scope of this policy. It is covered in the The Council 'Data Protection for Employee Data' policy.

3 Definitions

Employee

An individual who works part-time or full-time for The Council under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes temporary employees and independent contractors.

Customer
An external organisation with which The Council conducts business, that has contracted with The Council as a customer, and that has authorised The Council to have access to, and process, Personal Data for the purpose of conducting Internal Audits of both Financial data and Corporate Governance.

Personal Data
Any information (including opinions and intentions) which relates to an identified or Identifiable Living Person.

Contact
Any past, current or prospective The Council customer.

Identifiable Living Person
Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or one or more factors specific to the physical, economic, cultural or social identity of that living person.

Data Controller
A living person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. In our case, The Council.

Data Subject
The identified or Identifiable Living Person to whom the data refers.

Process, Processed, Processing
Any operation or series of operations performed on Personal Data. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or amendment, retrieval, consultation, use, disclosure and/or dissemination, restriction, erasure or destruction.

Data Protection
The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alternation, Processing, transfer or destruction.

Data Protection Authority
The independent public authority responsible for monitoring the application of the Data Protection regulation. The Council is registered with the Information Commissioner's Office under registration reference ZA336348.

Data Processor
A person, public authority, agency or other body that processes Personal Data on behalf of the Data Controller.

Consent

Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the Process of Personal Data relation to them.

Special Categories of Data
This includes data consisting of information pertaining to:

- Race of the data subject;
- Declared ethnicity of the data subject;
- Political opinions of the data subject;
- Religious beliefs of the data subject;
- Professed opinions or personal beliefs of the data subject;
- Membership of a Trades Union or other society;
- Physical and / or mental health or condition of the data subject;
- Sexual lifestyle of the data subject;
- The commission or alleged commission by the data subject of any offence; and
- Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

The Council and its employees are likely to have access to sensitive personal data rarely, if at all.

Personal Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored, or otherwise Processed.

Encryption
The process of converting information or data into code, to prevent unauthorised access.

Anonymisation
Data amended in such a way that no individuals can be identified from the data, whether directly or indirectly, by any means or by any person.

Confidential data
All data given in confidence, or data agreed to be kept confidential between the originator and The Council and that is not in the public domain.

Some confidential data will also be personal data and or sensitive personal data and therefore come within the terms of this policy. All The Council Employees will handle confidential data regularly as a function of the Auditing process.

4 Governance

Data Protection Officer
To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, The Council has appointed a suitably skilled Data Protection Officer.

Reporting to the Clerk and the Members of the Council, the Data Protection Officer's duties include:

- Advising The Council and its Employees who carry out Processing pursuant to Data Protection regulations;
- Ensuring the alignment of this policy with the General Data Protection Regulation;
- Undertaking Data Protection Impact Assessments (DPIAs);
- Acting as the point of contact for the Information Commissioner's Office;
- Maintaining a system that provides prompt and appropriate responses to Data Subject requests;
- Informing senior managers of any potential corporate, civil and/or criminal penalties which might be levied against The Council and/or its Employees for violation of applicable Data Protection Laws; and
- Establishing procedures and standard contractual provisions for obtaining compliance with this policy by any Employee Processing data on behalf of The Council.

Policy dissemination and enforcement

The Council management team continue to ensure that all Employees responsible for the Processing of Personal Data are aware of, and comply with, the contents of this policy.

Data Protection by design

To ensure that, as far as it is reasonably possible to do so, all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

A Data Protection Impact Assessment (DPIA) is conducted by the Data Protection Officer for all new and/or revised systems or processes. The subsequent findings of the DPIA must then be submitted to the Management team for review and approval. Likewise, IT systems and applications will be subject to continual review and annual impact assessments completed to assess the impact of any new technology uses on the security of Personal Data.

Compliance monitoring

To confirm that an adequate level of compliance is established and maintained by all The Council employees, the Data Protection Officer will carry out an annual Data Protection compliance audit which will assess:

- Compliance with The Council's Data Protection and Processing policies;
- Compliance with The Council's User Account policy; and,
- Compliance with The Council's Information Systems Security policy.

An annual training update will be given to all Employees

5 General Data Protection Regulation principles

Anyone Processing Personal Data must comply with the six data protection principles contained in the General Data Protection Regulation 2016 as they define how personal data can be legally processed: in summary these state that personal data shall:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and transparently in relation to the Data Subject. This means that other than in the case of data processed under the Local Audit and Accountability Act 2014, Regulation 5, for the purposes of statutory Internal Audits for Councils and Local Authorities, The Council must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness) and it must be for the purpose(s) specified in the applicable Data Protection regulation (Lawfulness).

The Local Audit and Accountability Act 2017 - Legal framework

The Local Audit and Accountability Act 2014, Regulation 5, provides auditors with a; "**right of access to all documents and files relating to a Council Audit that are considered necessary by those conducting the audit**." It is not a requirement to seek the personal consent of the individuals whose personal data is contained within documents or data in order to gain access to these for Internal Audit purposes.

Such documents and files include, but are not limited to, Accounting Systems back up files including cashbooks, financial reports, and associated spreadsheets, payroll records and employment contracts. Additionally, records of services provided to clients of the council are also reviewed. These may include allotment lease records, burial and memorial records, market stall fees records, facilities booking receipts, invoices and other similar items.

The Council processes 'personal data' for three reasons:

- For the purposes of conducting statutory Internal Audits on behalf of its Council clients: All data processed by The Council is anonymised and only used for reporting the Audit findings to the Client;
- To maintain Client relationships, it collects business address, email and telephone contract information, pertaining to The Council Clients, Prospective Clients and Business Contacts; and
- To recruit and pay its Employees.

The Council has conducted an extensive data impact audit and has categorised each type of data that it stores by risk and has implemented appropriate protocols to ensure the security of that data.

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means that The Council must specify exactly what the Personal Data Collected will be used for and limit the Processing of that Personal Data to only what is required to meet the specified Purpose.

Before commencing any Internal Audit, which will involve obtaining and/or processing personal data, the Auditor must give proper consideration to this policy and how it will be properly complied with.

In particular, Auditors must consider the type of personal data which is to be examined and the extent to which such data is legitimately required for the Audit process. All data and

the method used for its collection during the Internal Audit process is defined in the current year's Internal Audit Programme and must be recorded using the digital forms provided or by taking the hard or digital copies of documents that are required to support the Internal Audit conclusions.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. This means that The Council must not Store any Personal Data beyond what is absolutely required.

Personal data obtained or used during the Audit process is limited to the minimum amount of data which is reasonably required to achieve the Internal Audit objectives and all such personal data is anonymised so that data subjects cannot be identified.

Principle 4: Accuracy

Personal Data shall be accurate and current. This means that The Council must continue to maintain high quality processes for the identification and management of out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. All Personal Data Processed for the purposes of conducting Internal Audits for Councils, Local Authorities and such other bodies with whom contracts exist is held in anonymised format, is only retained for the minimum statutory period prescribed by Law after which it is securely deleted or disposed of. Further detail may be located in The Council's Document and Data Retention Policy.

Principle 6: Integrity & Confidentiality

Personal Data shall be 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. The Council continues to use appropriate technical and organisational measures to ensure that the integrity and confidentiality of Personal Data is maintained at all times.

Accountability

The Data Controller: The Council, shall be responsible for, and be able to demonstrate compliance with the General Data Protection Regulation. This means that The Council must demonstrate that the six Data Protection Principles, detailed above, are met for all Personal Data for which it is responsible.

6 Data Collection

Personal Data should be collected only from the Data Subject unless one of the following applies:

- The nature of the business purpose necessitates the collection of the Personal Data from other persons or bodies.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following applies:

- The Data Subject has received information by other means;
- The information must remain confidential due to a professional secrecy obligation; and,
- A national law expressly provides for the collection, Processing or transfer of the Personal Data. The Council is permitted to collect, Process and transfer data for the purposes of Internal Audit under the Local Audit and Accountability Act 2014, Regulation 5.

Where it has been determined that notification to a Data Subject is required, notification should occur, but in no case later than twenty-eight days.

7 Data Subject Consent

The Council will only obtain Personal Data by lawful and fair means, and where appropriate, with the knowledge and Consent of the individual concerned. Where the need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, The Council is committed to seeking such Consent.

The Data Protection Officer in cooperation with the Management team, has established a process for obtaining and documenting Data Subject Consent for the Collection, Processing, and/or transfer of their Personal Data. The process includes the provision for:

- Determining what disclosures should be made in order to obtain valid Consent;
- Ensuring that the request for consent is communicated in plain language in an intelligible and easily accessible form;
- Ensuring that Consent is freely given and not based on a conditional clause(s)
- Documenting the date, method and content of the disclosures made and the scope and validity of the Consent(s) given; and
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Data Subject notification

The Council will, when required by applicable law, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or Consent, such as The Council ability to collect, Process and transfer data for the purposes of Internal Audit under the Local Audit and Accountability Act 2014, Regulation 5; and
- The disclosures may be given electronically or in writing.

8 Data processing

The Council will only obtain Personal Data by lawful and fair means, and where appropriate with the knowledge and Consent of the individual concerned.

Data Use

The Council uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of The Council;
- To provide Internal Audit services to The Council customers; and
- The ongoing administration and management of customer services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by The Council to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that The Council would then provide their details for any other purpose.

The Council will Process Personal Data in accordance with the General Data Protection Regulation. More specifically, The Council will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes;
- Processing is necessary to undertake an Internal Audit on behalf of an The Council customer under the Local Audit and Accountability Act 2014, Regulation 5; and,
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

In any circumstance where Consent has not been gained for the specific Processing in question, The Council will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation

Personal data in the public domain

Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

The Council's practice is to make the following items of employee data freely available unless individuals have chosen to opt out.

- Names of directors and employees;
- Employees' workplace email addresses and telephone numbers;
- Employees' biographies and curriculum vitae from time to time;

- Employees names, academic and professional qualifications and memberships where appropriate; and
- Any additional information relating to Employees that they have agreed to be placed in the public domain, such as portrait photographs.

Similarly, as part of its regular business activities and auditing practice, The Council may process personal information about third parties that is already in the public domain where such process is carried out in accordance with the Local Audit and Accountability Act 2014 and the General Data Protection Regulation principles set out below and is unlikely to cause any damage or distress to the data subject.

Special Categories of Data

The Council does not Process Special Categories of Data (also known as sensitive data) described in section 3 'Definitions', under any circumstances whatsoever.

Data Quality

The Council will adopt all necessary measures to ensure the Personal Data that it collects, and Processes, is complete and accurate. The measures adopted by The Council to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, misleading or outdated, even where the Data Subject does not request rectification;
- Keeping Personal Data only for the period necessary to satisfy the permitted uses for Internal Audit purposes or applicable statutory retention period; and,
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

Digital Marketing

The Council does not undertake digital marketing, send unsolicited promotional or direct marketing material either electronically or via hard copy.

Data Retention

To ensure fair Processing, Personal Data will not be retained by The Council for longer than necessary in relation to the purposes for which it was originally collected, or for which it was Processed.

The length of time for which The Council needs to retain Personal Data is set out in the The Council Document and Data Retention Policy. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the Policy. All Personal Data will be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Keeping personal data properly secure is key in complying with the General Data Protection Regulation. All Employees are therefore responsible for ensuring that if they keep any personal data, it is kept securely and is not disclosed, either orally or in writing, intentionally or accidentally to any unauthorised third party.

The Council will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be subject.

The minimum set of security measures to be adopted by each The Council is provided in the The Council **Information Systems Security Policy**. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed;
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations;
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation;
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was accessed, modified on or removed from a data processing system;
- Ensure that Personal Data is protected against undesired destruction or loss;
- Ensure that Personal Data collected for different purposes can and is Processed separately; and
- Ensure that Personal Data is not kept longer than necessary.

9 Data Subject Requests

Individuals are entitled to see all information held about themselves, but personal data should only to be disclosed to third parties under specific conditions.

Wherever possible, The Council employees will be open with individuals in relation to information held about them. If an individual wants to make a formal Subject Access Request under the General Data Protection Regulation, they should be referred to the Data Protection Officer.

Data Subject Rights

The Data Subject has the right to:

- object to Processing of their Personal Data;
- lodge a complaint with the Data Protection Authority;
- request rectification or erasure of their Personal Data; and,
- request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Data Protection officer, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require The Council to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If The Council cannot respond fully to the request within 30 days, the Data Protection Officer shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request;
- Any information located to date;
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision;
- An estimated date by which any remaining responses will be provided; and
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).

Requests from persons representing the Data Subject

Caution will be exercised if employees are requested to disclose information about an individual to someone else, either within or outside The Council. Information may be passed on to other members of staff if it is legitimately required for the completion of an employee's Auditing duties, but in all other cases personal data may not be disclosed without the individual's consent. Even parents, spouses, friends, partners or sponsors are not entitled to information without the Data Subject's consent.

There are times when The Council may be required to pass personal information about an individual to a third party. Employees in the Human Resources department may legitimately disclose relevant data to appropriate third parties to meet statutory requirements. The employee dealing with the request will need to be satisfied as to the legitimacy of the enquirer's identity and request.

The Council may also receive requests for information from bodies such as the police and HMRC. Any information disclosure will only take place after The Council has satisfied itself, to the extent that it is reasonably possible to do so, that any request made is genuine and legitimate.

Disclosing information in an emergency

Personal information can be disclosed in an emergency. In such a situation, if necessary, personal information can be disclosed without consent. For example, if an employee collapses and is unconscious, it would be permissible to inform medical staff that the individual suffers from a medical condition.

No information about an individual will be disclosed to any other enquirers, without written and signed permission from the individual to release their personal data.

Complaints handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is both reasonable and proportionate. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office.

Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail clerk@llantrisant-cc.gov.wales

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will report the Personal Data Breach to the Information Commissioner's Office and advise the parties affected.

10 Responsibilities of Employees

All Employees must:

- Be mindful of the fact that individuals have the right to see their 'personal data'. This may include, but is not limited to, applications for employment submitted by prospective Auditors, or comments written about people in e-mails. No comments or other data should be recorded about individuals which the author would not be comfortable in the individual seeing or being informed of;
- Report immediately the loss or theft of any personal data, contained in a printed document, on a mobile device or storage tool such as a controlled memory stick laptop or similar, to the Clerk, who is the Data Protection Officer;
- Report immediately to the Clerk if they find any lost or discarded data that they believe contains personal data contained in a printed document, on a mobile device or storage tool such as USB stick or laptop or similar;
- Maintain the contents of all personal data which comes into their possession securely and in accordance with The Council's written policies;
- Ensure that all personal data that is provided by them, to The Council is accurate;
- Notify The Council expeditiously of any changes to their own personal data, i.e. change of address or emergency contact details;
- Only ever obtain and or use personal data relating to third parties for approved auditing purposes;
- Ensure that all personal data processed is done so in accordance with the requirements of the General Data Protection Regulation 2016;
- Familiarise themselves with The Council's General Data Protection Regulation Policy and comply with it at all times;
- Familiarise themselves with The Council's Remote Working & Mobile Computing Policy and IT Security Policy and comply with them at all times; and,

- Seek advice of the Data Protection Officer whenever you are unsure as to how to process personal data or if you have any data protection concerns whatsoever.

Prohibited activities

The following activities are strictly prohibited:

- Using data obtained for one purpose for another supplemental purpose; i.e. using contact details provided for Human Resources purposes for marketing initiatives; and,
- Disclosing personal data to a third party outside of The Council without the consent of the data subject.

Implications of breaching this policy

It is a condition of employment in the case of all employees that they will abide by the policies and rules of The Council. Any breach of this policy will be considered a disciplinary offence and may lead to disciplinary action, and/or the individual being held liable in law.

11 Conclusion

Compliance with the General Data Protection Regulation (GDPR) EU 2016/679 which comes into force on the 25th May 2018 is the responsibility of all members of The Council, and any questions about this policy or concerning data protection matters should be raised with the Data Protection Officer at clerk@llantrisant-cc.gov.wales .

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version number	Version 1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

DATA MAINTAINED BY AUDITING SOLUTIONS			
Data Category	Data Type	Contains Personal Data	Sensitivity level (High/Medium/Low)
ASL employees	Employment contracts	Yes	High
	Leave/sickness record	Yes	High
	Discipline/Grievance record	Yes	High
	Next of Kin details	Yes	Low
	Accident/Injury record	Yes	High
	Pension details	Yes	High
	PAYE	Yes	Low
	Contact details	Yes	Medium
	Bank details	Yes	High
	Job applications	Yes	Low
	References	Yes	Low
	Staff Appraisals	Yes	Medium
	Performance Plans	Yes	Medium
Third Parties/ Customers	Address details	No	Low
	Email Addresses	No	Low
Engagement & Contact	Quotations	No	Low
	Contract of Engagement	No	Low
	Complaints	Yes	Medium
	Freedom of Information requests	Yes	High
	Subject Access requests	Yes	High
Third Parties/ Customers	Digital or hard copy cashbooks	Yes	High
	Bank Statements	Yes	High

Audit	Building Society Statements	Yes	High
	Term Deposit statements	No	High
	Cheque Books	Yes	High
	Electronic payment reports	Yes	High
	VAT reports	No	Low
	Journal reports	Yes	High
	Standing Orders	No	Low
	Financial Regulations	No	Low
	External Auditor's Report	No	Low
	Council & Committee minutes (gen)	No	Low
	Staffing Committee minutes	Yes	High
	Corporate Governance Questionnaire	No	Low
	Purchase Orders	No	Low
	Payment Invoices	No	Low
	Payment & Salary Tester	No	Low
	Grants & Donations	No	Low
	Expense Claim forms	No	Low
	Financial Risk Register	No	Low
	Health & Safety Risk Register	No	Low
	Operations Management Risk Regsiter	No	Low
	Insurance policy/policies	No	Low
	Playground reports - internal	No	Low
	Playground reports - Independent	No	Low
	Budget reports	No	Low
	Precept determination budget	No	Low
	Earmarked Reserve documentation	No	Low
	Reserve Funds reports	No	Low
	Variance reports	No	Low
	Sales Ledger files	Yes	Medium
	Sales Receipts	No	Low
	Paying In Books	Yes	High
	Sales Invoices	No	Low

	Burials Register	No	Low
	Memorials Register	Yes	Medium
	Allotments Register	Yes	Medium
	Lease Agreements	Yes	Medium
	Petty Cash reconciliations	No	Low
	Petty Cash	No	Low
	Petty Cash receipts	No	Low
	Debit/Credit Card statements	No	Low
	Staff establishment list	Yes	High
	Staff contracts	Yes	High
	Staff Pay Award details	Yes	High
	Payroll reports	Yes	High
	HMRC RTI reports	Yes	High
	HMRC Tax Code documents	Yes	High
	Staff Pay Slips	Yes	High
	Time Sheets / Overtime Approval	Yes	High
	Pension Reports	Yes	High
	Asset Register	No	Low
	Loans acquired	No	Low
	Loans issued	Yes	High
	Investments	No	Low
	Bank reconciliations	No	Low
	Building Socieity reconciliations	No	Low
	Investment Fund reconciliations	No	Low
	Annual Analytical Review	No	Low
	S.137 Reports	No	Low
	Annual Return Data	No	Low
	AGAR	No	Low
	IA Programme	No	Low
	Internal Audit Report	No	Low

Page 17 of 74

Page 18 of 74

LAWFUL BASIS FOR DATA RETENTION						
Data Category	Data Type	Purpose	Data Function	Legal obligation to hold data	Legal basis for Data retention	Consent or prevaling legislation
ASL employees	Employment contracts	HR	Legislative	Yes	Contract	Yes
	Leave/sickness record	HR	Legislative	Yes	Employment Law	Legislation
	Discipline/Grievance record	HR	Employment records	Yes	Employment Law	Legislation
	Next of Kin details	HR	Employment records	No	Contract	Yes
	Accident/Injury record	HR	Health & Safety	Yes	H&S Legislation	Legislation
	Pension details	HR	Legislative	Yes	HMRC	Legislation
	PAYE	HR	Legislative	Yes	HMRC	Legislation
	Contact details	HR	Employment records	No	Contract	Yes
	Bank details	HR	Employment records	No	Contract	Yes
	Job applications	HR	Employment records	No	Contract	Yes
	References	HR	Employment records	No	Contract	Yes
	Staff Appraisals	HR	Employment records	No	Employment Law	Legislation
	Performance Plans	HR	Employment records	No	Employment Law	Legislation
Third Parties/ Customers	Address details	Management	Business Operations	No	Contract	Not required
	Email Addresses	Management	Business Operations	No	Contract	Not required
Engagement & Contact	Quotations	Management	Business Operations	No	Contract	Not required
	Contract of Engagement	Management	Business Operations	No	Contract	Not required
	Complaints	Management	Business Operations	No	Contract	Not required
	Freedom of Information requests	Management	Business Operations	Yes	GDPR EU 2016/679	Not required
	Subject Access requests	Management	Business Operations	Yes	GDPR EU 2016/679	Not required
Third Parties/ Customers Audit	Digital or hard copy cashbooks	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5
	Bank Statements	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5
	Building Society Statements	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5

	Term Deposit statements	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5
	Cheque Books	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5
	Electronic Payment records	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5
	VAT reports	Audit	Payments Procedures	No	Contract	LAAA 2017, Reg 5
	Journal reports	Audit	Accounting Records	No	Contract	LAAA 2017, Reg 5
	Standing Orders	Audit	Corporate Governance	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Financial Regulations	Audit	Corporate Governance	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	External Auditor's Report	Audit	Corporate Governance	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Council & Committee minutes (gen)	Audit	Corporate Governance	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Staffing Committee minutes	Audit	Corporate Governance	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Corporate Governance Questionnaire	Audit	Corporate Governance	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Purchase Orders	Audit	Payments Procedures	No	Contract	LAAA 2017, Reg 5
	Payment Invoices	Audit	Payments Procedures	No	Contract	LAAA 2017, Reg 5
	Payment & Salary Tester	Audit	Payments Procedures	No	Contract	LAAA 2017, Reg 5
	Grants & Donations	Audit	Payments Procedures	No	Contract	LAAA 2017, Reg 5
	Expense Claim forms	Audit	Payments Procedures	No	Contract	LAAA 2017, Reg 5
	Financial Risk Register	Audit	Assessment & Management of Risk	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Health & Safety Risk Register	Audit	Assessment & Management of Risk	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Operations Management Risk Regsiter	Audit	Assessment & Management of Risk	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Insurance policy/policies	Audit	Assessment & Management of Risk	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Playground reports - internal	Audit	Assessment & Management of Risk	No	Contract	LAAA 2017, Reg 5
	Playground reports - Independent	Audit	Assessment & Management of Risk	No	Contract	LAAA 2017, Reg 5
	Budget reports	Audit	Budget setting & Precept determination	No	Contract	LAAA 2017, Reg 5
	Precept determination budget	Audit	Budget setting & Precept determination	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Earmarked Reserve documentation	Audit	Budget setting & Precept determination	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Reserve Funds reports	Audit	Budget setting & Precept determination	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Variance reports	Audit	Budget setting & Precept determination	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Sales Ledger files	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Sales Receipts	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Paying In Books	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Sales Invoices	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Burials Register	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Memorials Register	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Allotments Register	Audit	Income Control	No	Contract	LAAA 2017, Reg 5

	Lease Agreements	Audit	Income Control	No	Contract	LAAA 2017, Reg 5
	Petty Cash reconciliations	Audit	Petthy Cash records & Credit/Debit cards	No	Contract	LAAA 2017, Reg 5
	Petty Cash	Audit	Petthy Cash records & Credit/Debit cards	No	Contract	LAAA 2017, Reg 5
	Petty Cash receipts	Audit	Petthy Cash records & Credit/Debit cards	No	Contract	LAAA 2017, Reg 5
	Debit/Credit Card statements	Audit	Petthy Cash records & Credit/Debit cards	No	Contract	LAAA 2017, Reg 5
	Staff establishment list	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Staff contracts	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Staff Pay Award details	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Payroll reports	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	HMRC RTI reports	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	HMRC Tax Code documents	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Staff Pay Slips	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Time Sheets / Overtime Approval	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Pension Reports	Audit	Salaries & Wages	No	Contract	LAAA 2017, Reg 5
	Asset Register	Audit	Asset Register(s)	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Loans acquired	Audit	Investments & Loans	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Loans issued	Audit	Investments & Loans	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Investments	Audit	Investments & Loans	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Bank reconciliations	Audit	Bank Reconciliations	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Building Socieity reconciliations	Audit	Bank Reconciliations	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Investment Fund reconciliations	Audit	Bank Reconciliations	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Annual Analytical Review	Audit	Financial Statements	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	S.137 Reports	Audit	Financial Statements	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Annual Return Data	Audit	Financial Statements	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	AGAR	Audit	Financial Statements	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	IA Programme	Audit	Business Operations	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5
	Internal Audit Report	Audit	Financial Statements	Yes	LAAA 2017, Reg 5	LAAA 2017, Reg 5

THIRD PARTY DATA ACCESS		
Data Category	**Data Type**	**Third Parties with which data is shared**
Staff	Employment contracts	External Professional Advisers
	Leave/sickness record	External Professional Advisers, HMRC
	Discipline/Grievance record	External Professional Advisers
	Next of Kin details	Not shared
	Accident/Injury record	External Professional Advisers
	Pension details	External Professional Advisers, HMRC
	PAYE	External Professional Advisers, HMRC
	Contact details	External Professional Advisers HMRC
	Bank details	Not shared
	Job applications	Not shared
	References	Not shared
	Staff Appraisals	External Professional Advisers in the event of dispute
	Performance Plans	External Professional Advisers in the event of dispute
Third Parties/ Customers	Address details	Public domain
	Email Addresses	Public domain
	Quotations	Public domain
Engagement & Contact	Contract of Engagement	Not shared
	Complaints	External Professional Advisers
	Freedom of Information requests	External Professional Advisers in the event of dispute
	Subject Access requests	External Professional Advisers in the event of dispute
Third Parties/	Digital or hard copy cashbooks	Not shared

Customers	Bank Statements	Not shared
Audit	Building Society Statements	Not shared
	Term Deposit statements	Not shared
	Cheque Books	Not shared
	Electronic Payment records	Not shared
	VAT reports	Not shared
	Journal reports	Not shared
	Standing Orders	Public domain
	Financial Regulations	Public domain
	External Auditor's Report	Public domain
	Council & Committee minutes (gen)	Public domain
	Staffing Committee minutes	Not shared
	Corporate Governance Questionnaire	Public domain
	Purchase Orders	Not shared
	Payment Invoices	Not shared
	Payment & Salary Tester	Not shared
	Grants & Donations	Not shared
	Expense Claim forms	Not shared
	Financial Risk Register	Not shared
	Health & Safety Risk Register	Not shared
	Operations Management Risk Regsiter	Not shared
	Insurance policy/policies	Not shared
	Playground reports - internal	Not shared
	Playground reports - Independent	Not shared
	Budget reports	Not shared
	Precept determination budget	Not shared
	Earmarked Reserve documentation	Not shared
	Reserve Funds reports	Not shared
	Variance reports	Not shared
	Sales Ledger files	Not shared
	Sales Receipts	Not shared
	Paying In Books	Not shared

	Sales Invoices	Not shared
	Burials Register	Not shared
	Memorials Register	Not shared
	Allotments Register	Not shared
	Lease Agreements	Not shared
	Petty Cash reconciliations	Not shared
	Petty Cash	Not shared
	Petty Cash receipts	Not shared
	Debit/Credit Card statements	Not shared
	Staff establishment list	Not shared
	Staff contracts	Not shared
	Staff Pay Award details	Not shared
	Payroll reports	Not shared
	HMRC RTI reports	Not shared
	HMRC Tax Code documents	Not shared
	Staff Pay Slips	Not shared
	Time Sheets / Overtime Approval	Not shared
	Pension Reports	Not shared
	Asset Register	Not shared
	Loans acquired	Not shared
	Loans issued	Not shared
	Investments	Not shared
	Bank reconciliations	Not shared
	Building Society reconciliations	Not shared
	Investment Fund reconciliations	Not shared
	Annual Analytical Review	Not shared
	S.137 Reports	Not shared
	Annual Return Data	Not shared
	AGAR	External Auditor appointed to the customer
	Internal Audit Report	Not shared
	Internal Audit Report	Public domain

Data Protection Impact Assessment

10th December 2024

LLANTRISANT COMMUNITY COUNCIL DATA MANAGEMENT						
Data Category	**Data Type**	**Data custodian**	**Data Review cycle**	**Data Retention period**	**Data Location**	**Data Security**
Staff	Employment contracts	Clerk	On appointment	Duration of Employment plus 6 years	Server/Secure filing cabinet	Password & lock and key
	Leave/sickness record	Clerk	As required	End of Financial year plus one year	Server/Secure filing cabinet	Password & lock and key
	Discipline/Grievance record	Clerk	As required	Duration of Employment plus 6 years	Server/Secure filing cabinet	Password & lock and key
	Next of Kin details	Clerk	As required	Duration of Employment plus 6 years	Server/Secure filing cabinet	Password & lock and key
	Accident/Injury record	Clerk	As required	Duration of Employment plus 6 years	Server/Secure filing cabinet	Password & lock and key
	Pension details	Clerk	As required	Duration of Employment plus 6 years	Server/Secure filing cabinet	Password & lock and key
	PAYE	Clerk	monthly	Duration of Employment plus 6 years	Server/Secure filing cabinet	Password & lock and key
	Contact details	Clerk	As required	Duration of employment	Server/Secure filing cabinet	Password & lock and key
	Bank details	Clerk	Upon request	Duration of employment	Server/Secure filing cabinet	Password & lock and key
	Job applications	Clerk	On application	Until appointment made	Server/Secure filing cabinet	Password & lock and key
	References	Clerk	On offer	Duration of employment	Server/Secure filing cabinet	Password & lock and key
	Staff Appraisals	Clerk	Annually	Duration of employment	Server/Secure filing cabinet	Password & lock and key
	Performance Plans	Clerk	As required	Duration of employment	Server/Secure filing cabinet	Password & lock and key
Third Parties/ Customers	Address details	Clerk	As required	Duration of Contract	Server	Password
	Email Addresses	Clerk	As required	Duration of Contract	Server	Password
Engagement & Contact	Quotations	Clerk	As required	Duration of Contract	Server	Password
	Contract of Engagement	Clerk	As required	Duration of Contract	Server/Secure filing cabinet	Password & lock and key
	Complaints	Clerk	As required	Duration of Contract	Server/Secure filing cabinet	Password & lock and key
	Freedom of Information requests	Clerk	As required	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Subject Access requests	Data Protection Officer	As required	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
Third Parties/ Customers Audit	Digital or hard copy cashbooks	Assigned employee	Audit frequency	Document & Data Retention policy	Server	Password
	Bank Statements	Assigned employee	On appointment	Document & Data Retention policy	Secure filing cabinet	Password & lock and key
	Building Society Statements	Assigned employee	On appointment	Document & Data Retention policy	Secure filing cabinet	Password & lock and key
	Term Deposit statements	Assigned employee	Audit frequency	Document & Data Retention policy	Secure filing cabinet	Password & lock and key
	Cheque Books	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Electronic Payment records	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	VAT reports	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Journal reports	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Standing Orders	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Financial Regulations	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	External Auditor's Report	Assigned employee	Annually	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key

	Council & Committee minutes (gen)	Assigned employee	Audit frequency	Document & Data Retention policy	Server	Password
	Staffing Committee minutes	Assigned employee	Audit frequency	Document & Data Retention policy	Server	Password
	Corporate Governance Questionnaire	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Purchase Orders	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Payment Invoices	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Payment & Salary Tester	Assigned employee	Audit frequency	Document & Data Retention policy	Server	Password
	Grants & Donations	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Expense Claim forms	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Financial Risk Register	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Health & Safety Risk Register	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Operations Management Risk Regsiter	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Insurance policy/policies	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Playground reports - internal	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Playground reports - Independent	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Budget reports	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Precept determination budget	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Earmarked Reserve documentation	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Reserve Funds reports	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Variance reports	Assigned employee	Annually	Document & Data Retention policy	Server	password
	Sales Ledger files	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Sales Receipts	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Paying In Books	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Sales Invoices	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Burials Register	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Memorials Register	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Allotments Register	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Lease Agreements	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Petty Cash reconciliations	Assigned employee	Annually	Document & Data Retention policy	Server	Password
	Petty Cash	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Petty Cash receipts	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Debit/Credit Card statements	Assigned employee	Audit frequency	Document & Data Retention policy	Not retained	N/A
	Staff establishment list	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Staff contracts	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Staff Pay Award details	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Payroll reports	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	HMRC RTI reports	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	HMRC Tax Code documents	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Staff Pay Slips	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Time Sheets / Overtime Approval	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A
	Pension Reports	Assigned employee	Annually	Document & Data Retention policy	Not retained	N/A

	Asset Register	Assigned employee	Annually	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Loans acquired	Assigned employee	Audit frequency	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Loans issued	Assigned employee	Audit frequency	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Investments	Assigned employee	Audit frequency	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Bank reconciliations	Assigned employee	Audit frequency	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Building Socieity reconciliations	Assigned employee	Audit frequency	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Investment Fund reconciliations	Assigned employee	Audit frequency	Document & Data Retention policy	Server/Secure filing cabinet	Password & lock and key
	Annual Analytical Review	Clerk	Annually	Document & Data Retention policy	Server	Password
	S.137 Reports	Clerk	Annually	Document & Data Retention policy	Server	Password
	Annual Return Data	Clerk	Annually	Document & Data Retention policy	Server	Password
	AGAR	Clerk	Annually	Document & Data Retention policy	Server	Password
	Internal Audit Report	Clerk	Annually	Document & Data Retention policy	Server	Password

Page 27 of 74

LLANTRISANT COMMUNITY COUNCIL RISK ANALYSIS					
Subject	**Risk Identified**	**High / Medium / Low Risk**	**Management Control of Risks**	**Review / Assess / Revise**	**Next Review date**
GDPR	Non compliance with GDPR / Damage to business reputation / business interruption / fine	L	Council has undertaken a full data impact assessment and developed policies, procedures and employee training to ensure compliance with GDPR	Existing procedures adequate	DEC 2024
Data Protection	Non compliance with GDPR	L	Council is registered with the ICO and acts on all guidance published as soon as it is practicably possible to do so.	Existing procedures adequate	DEC 2024
Freedom of Information	Non compliance with GDPR / Damage to business reputation / business interruption / fine	L	Council has a model publication scheme in place. FoI requests are managed by the Data Protection Officer and is aware that such requests may require additional time and resources.	Existing procedures adequate	DEC 2024
Data Breach	Non compliance with GDPR / Damage to business reputation / business interruption / fine	M	Council is in the process of implementing a server based IS Solution using Microsoft Office 365 which will allow Employees to work against the files on the Corporate server rather than download them to encrypted drives or memory sticks	IS implementation to be completed by July 2018.	DEC 2024
Data Loss (Electronic)	Non compliance with GDPR / Damage to business reputation / business interruption / fine	L	Council provides all employess with encrypted memory sticks for remote working at Client sites and from home offices. Formal Remote Working Policy in place which requires the immediate reporting of any Loss of Data	Existing procedures adequate	DEC 2024
Data Loss (Paper)	Non compliance with GDPR / Damage to business reputation / business interruption / fine	L	Council has a robust Remote Working Policy in place. All employees receive training about data security and remote working practices and are contractually obliged to abide by the Remote Working Policy.	Existing procedures adequate	DEC 2024
Data Loss (systems failure)	Non compliance with GDPR / Damage to business reputation / business interruption	M	Current systems are reliant on individuals to take responsibility for Data Security and Back up. However, Council is in the process of implementing a new server based cloud system using Microsoft 365 where all files will be automatically backed up on to a corporate data cloud using Office 365. The data farm is located in the Republic of Ireland and within the EU's list of approved countries.	New procedures and systems in the process of implementation.	DEC 2024
Data Loss (virus / malware attack)	Non compliance with GDPR / Damage to business reputation / business interruption	M	Current systems are reliant on individuals to take responsibility for Antivirus and Malware software. However, Council is in the process of implementing a new server based cloud system using Microsoft 365 where all files will be automatically backed up on to a corporate data cloud using Office 365. The data farm is located in the Republic of Ireland and within the EU's list of approved countries.	New procedures and systems in the process of implementation.	DEC 2024
Unauthorised Access internal	Potential non compliance with GDPR / Damage to business reputation / fine	L	All employees have access ONLY to data pertaining to the Clients that have been assigned to them for the purposes of Internal Audit. The Source data is maintained and managed on the Corporate Server which is password protected with the company's directors having administration rights. All employee accounts are password protected and can be remotely locked if any suspicious activity is detected.	Existing procedures adequate	DEC 2024
Unauthorised Access external	Non compliance with GDPR / Damage to business reputation / business interruption	L	Clerk does not public IT interfaces with its servers. Additionally, it is a SME providing a niche service to a limited market, so unlikely to attract the attentions of hackers or spamers.	Existing procedures adequate	DEC 2024

Page 28 of 74

Inappropriate handling of client data	Potential non compliance with GDPR / Damage to business reputation / fine	L	Clerk provides detailed training to its employees and requires that standardised Audit Programmes and data collection tools are used during the audit process. The programmes and supporting files are subject to annual review by the management team to ensure compliance with all relevant legislation.	Existing procedures adequate.	DEC 2024
Destruction of Council employee data	Non compliance with GDPR / Non Compliance with employment law / business interruption / fine	L	Employee data and documents are retained at Council's Head Office on a secure server and in a locked filing cabinet. The Server is backed up on a daily basis. Upon implementation of the new Council corporate IS platform all data will be immediately saved to the secure corporate cloud which has several mirrored backups and will be subject to a higher level of security.	Existing procedures adequate.	DEC 2024
Freedom of Information request handling	Non compliance with the FoI act, GDPR and damage to business retputation	L	FoI requests are handled by the <<CLERK>> and the Data Protection Officer who are both aware of the requirements of FoI requests and the time required to properly respond to any such request.	Existing procedures adequate.	DEC 2024
Subject Access request handling	Potential non compliance with GDPR / Damage to business reputation / fine	L	Subject Access requests are handled by the Data Protection Officer with oversite of the <<CLERK>>. Both aware of the requirements of Subject Access requests under GDPR and the time required to properly respond to any such request.	Existing procedures adequate.	DEC 2024
Complaints handling	Potential non compliance with GDPR / Damage to business reputation	L	Complaints are handled by the <<CLERK>> (Data Protection Officer if required). Both are aware of the time required to properly respond to any such request.	Existing procedures adequate.	DEC 2024
Client's Accounts Systems Backup	Potential non compliance with GDPR / Damage to business reputation / fine	L	Client's Accounts systems backups and spreadsheet cashbooks both contain details of salary payments which are considered sensitive data. Accounts Systems backups and cashbooks are i) only shared with the employee responsible for the Client Audit; and, 2) are maintained in a password protected format; and 3) only retained until the external auditors' reports for the corresponding financial year have been issued at which time they are securely deleted. Policies and procedures are in place governing the management of Client data and employees receive induction and annual update training.	Existing procedures adequate	DEC 2024
Client's Bank/Building Society/Funds statements	Potential non compliance with GDPR / Damage to business reputation	L	Bank statements and corresponding documents from similar instituations contain details of account numbers, sort codes and IBAN numbers which may be used to access the Client's funds contained therein. Copies of the original statements are NOT retained. Information concerning opening and closing balances are recrorded in the internal Council IA Programme.	Existing procedures adequate.	DEC 2024
Staffing Committee meeting minutes	Potential non compliance with GDPR / Damage to business reputation / fine	L	Staffing Committee meeting minutes may contain details of confidential matters such as recruitment, pay awards, grievances and appraisals etc., Such data is highly sensitive. Council auditors are required as a function of the Internal Audit process to review such minutes. Copies of confidential minutes are NOT retained. The review of minutes recorded on internal form Council 2.2 and the IA programe where all confidential matters are anonymised.	Existing procedures adequate.	DEC 2024

Payroll, PAYE and Pension data	Potential non compliance with GDPR / Damage to business reputation / fine	L	All payroll related information is highly sensitive. Council auditors are required as a function of the Internal Audit process to review data relation to identification of the correct rate of pay, including variable hours and PAYE/NIC/Pension and other statutory deductions made by the Client. No original documents are retained by Council and anonymised data only collected in internal Form Council 8.2. Any findings are recorded on the Council IA programme and are again anonymised. All Council employees receive induction and update training concerning the collection and analysis of this data.	Existing procedures adequate.	DEC 2024
Loans issued	Potential non compliance with GDPR / Damage to business reputation / fine	L	Loans issued by Clients are often, but not always, issued to members of staff. In such cases, the information is treated as highly sensitive. Council auditors are required as a function of the Internal Audit process to review data relation to loans issued. Findings are recorded in anonymised format on the Council IA Programme. All Council employees receive induction and update training concerning the collection and analysis of this data.	Existing procedures adequate.	DEC 2024
Inappropriate/ irrelevant Client data retained and collected	Potential non compliance with GDPR / Damage to business reputation / fine		Council does not maintain original client data for and on behalf of its clients. It only holds the data that has been necessary to collect for the purposes of conducting a proper Internal Audit and to allow the Internal Audit Report in Annual Governance and Accountability Returns for Council's to be completed. All Audits are conducted using the approved Council IA programme for the corresponding financial year. The Council IA Programme is reviewed and revised on an annual basis and reissued to employees by the managment team prior to audits in the corresponding financial year being undertaken.	Existing procedures adequate.	DEC 2024
Client data retained for longer than required	Potential non compliance with GDPR / Damage to business reputation / fine	L	Council has an approved Document and data retention policy that specifies the length of time which all documents and data are retained for prior to secure destruction. An annual audit is conducted in March to ensure that this policy is strictly adhered to.	Existing procedures adequate.	DEC 2024
Client data destroyed	Potential non compliance with GDPR / Damage to business reputation	L	Council does not maintain original client data for and on behalf of its clients. It only holds the data that has been necessary to collect for the purposes of conducting a proper Internal Audit and to allow the Internal Audit Report in Annual Governance and Accountability Returns for Council's to be completed. All Audits are conducted using the approved Council IA programme for the corresponding financial year. The Council IA Programme is reviewed and revised on an annual basis and reissued to employees by the managment team prior to audits in the corresponding financial year being undertaken.	Existing procedures adequate.	DEC 2024
Data subject consent	Potential non compliance with GDPR / Damage to business reputation / fine	L	Council is committed to seeking Data Subject Consent to Process all data where it is required to do so. However, Council and its employees, acting in the capacity of Internal Auditors to Council's is provided by the Local Audit and Accountability Act 2017, Regulation 5 with a "right of access to all documents and files relating to a Council Audit that are considered necessary by those conducting the Audit". As such it does not need to seek consent to access or review personal data required by the audit process and which is prescribed in the Council IA programme.	Existing procedures adequate.	DEC 2024
Purpose Liitation	Potential non compliance with GDPR / Damage to business reputation / fine	L	Personal data is only collected for specified, explicit and legitimate purposes of Internal Audit as detailed in the Council IA Programme.	Existing procedures adequate.	DEC 2024

Data Minimisation	Potential non compliance with GDPR / Damage to business reputation / fine	L	Personal data is adequate, relevant and limited only to what is necessary in relation to the legitimate purposes of Internal Audit as detailed in the Council IA Programme.	Existing procedures adequate.	DEC 2024
Accuracy	Potential non compliance with GDPR / Damage to business reputation / fine	L	Personal data reviewed is current to the financial year of the corresponding audit and only utilised for the legitimate purposes of Internal Audit as detailed in the Council IA Programme.	Existing procedures adequate.	DEC 2024
Storage Limitation	Potential non compliance with GDPR / Damage to business reputation / fine	L	Personal data is anonymised and stored in the Council IA Programme and supporting files is stored only for the period prescribed in the Council Document and Data Retention Policy. Upon reaching the retention limit such data is securely deleted/destroyed.	Existing procedures adequate.	DEC 2024
Integrity & Confidentiality	Potential non compliance with GDPR / Damage to business reputation / fine	L	Personal data is processed only in a manner that ensures appropriate security of the Personal Data as prescribed in the Council IA Programme.	Existing procedures adequate.	DEC 2024
Accountability	Potential non compliance with GDPR / Damage to business reputation / fine	L	Council has taken all reasonble steps to comply with the General Data Protection Regulation and can demonstrate that it meets the requirements of the six Data Protection Principles. Council has appointed a Data Protection Officer to oversee the company's continue compliance with GDPR.	Existing procedures adequate.	DEC 2024
Employee responsibilities	Potential non compliance with GDPR / Damage to business reputation / fine	L	It is a condition of employment in the case of all employees that they will abide by the policies and rules of Clerk. Any breach of this policy will be considered a disciplinary offience, and / or the individual being held liable in law.	Existing procedures adequate.	DEC 2024

IT Acceptable Use Policy

What you are permitted and prohibited from doing when you use Llantrisant Community Council's IT systems and the consequences of breaking the rules

Introduction

All users of the Council' infrastructure and facilities are bound by the provisions of its policies in addition to this Acceptable Use Policy. Llantrisant Community Council seeks to promote and facilitate the positive use of Information Technology in the interests of supporting the delivery of Auditing services and consultancy to the highest standards. This also requires appropriate and legal use of the technologies and facilities made available to Staff and third parties.

Unacceptable Use

Llantrisant Community Council's infrastructure may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of;

1) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2) unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3) unsolicited "nuisance" emails;
4) material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Llantrisant Community Council team or a third party;
5) material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6) material with the intent to defraud or which is likely to deceive a third party;
7) material which advocates or promotes any unlawful act;
8) material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9) material that brings Llantrisant Community Council, into disrepute.

Llantrisant Community Council's network must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:

1) intentionally wasting staff effort or other Llantrisant Community Council's resources;
2) corrupting, altering or destroying another user's data without their consent;
3) disrupting the work of other users or the correct functioning of Llantrisant Community Council's network; or
4) denying access to the Llantrisant Community Council's network and its services to other users.
5) pursuance of private commercial activities not related to Llantrisant Community Council.

6) introduce data-interception, password-detecting or similar software or devices to the Llantrisant Community Council Network.
7) seek to gain unauthorised access to restricted areas of the Council' Network;
8) access or try to access data where the user knows or ought to know that they should have no access;
9) carry out any hacking activities or intentionally or recklessly introduce any form of spyware, computer virus or other malicious software.

If a member of the Llantrisant Community Council community believes they may have encountered breaches of any of the above, they should immediately make this known to the Data Protection Officer, Clerk@llantrisant-cc.gov.wales

Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a user, Llantrisant Community Council may at its sole discretion:

a) restrict or terminate a user's right to use the Llantrisant Community Council Network;
b) withdraw or remove any material uploaded by that user in contravention of this Policy; or
c) where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith. In addition, where the user is also a Llantrisant Community Council staff member or third party, Llantrisant Community Council may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with Contract and Statute.

Definitions

Llantrisant Community Council Network – all computing, telecommunication, and networking facilities provided by the Llantrisant Community Council with particular reference to all computing devices, either personal or Llantrisant Community Council's owned, connected to systems and services supplied by Llantrisant Community Council.

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version Number	Version 1.0
Original approval date	10/12/2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	2018
Date of next review	2028

Digital Information Systems Security Policy

Our responsibilities for ensuring the security of information systems at Llantrisant Community Council

1 Introduction

The continued confidentiality, integrity and availability of information systems underpin the operations of Llantrisant Community Council. A failure to secure information systems would jeopardise the ability of the Council to fulfil its Auditing function and have greater long-term impact through the consequential risk of financial or reputational loss.

The Management team are committed to delivering and successfully implementing Information Security Management, but this is only possible if all staff and third parties are aware of, and carry, out their own personal responsibilities.

This Digital Information Systems Security policy provides the guiding principles and responsibilities of all members of the Council, its Staff and third parties required to safeguard its information systems. Other supporting policies give greater detail on specific subject areas.

1.1 Purpose of Policy

The intention of this policy is to:

- Ensure that the Council's information systems are protected from security threats and to mitigate risks that cannot be directly countered;
- Ensure that all 's staff and third parties are aware of, and are able to comply with relevant UK and EU legislation;
- Ensure that the Council staff and third parties are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access;
- Ensure that all users are aware of and comply with this and other supporting policies.
- Safeguard the reputation and business of the Council by ensuring its ability to meets its legal obligations and to protect it from liability or damage through misuse of its IT facilities

- Ensure timely review of policy and procedure in response to feedback, legislation and other factors so as to improve ongoing security.

1.2 Scope

This Information Systems Security Policy applies to all the Council's staff and third parties who interact with the Council's data, the data of its Clients, and all of the systems used to store or process it.

2 Policy

2.1 Awareness and communication

All authorised users will be informed of the policy and of supporting policies and guidelines when commencing employment, contracting or subcontracting with the Council. Updates to guidance will be publicised through the Company's website, highlighted at the bi-annual team meeting and in e-mail bulletins which may be issued from time to time.

2.2 Definitions

The Council' Data's - This includes all data elements that are owned or licenced by the Council or any information processed by the company on behalf of its clients.

The Council's information systems - This includes but is not limited to all information systems owned, held, utilised or present on the Council's network, and anyone making use of them.

Data Protection Officer – This person is ultimately responsible for data management, retention and security.

Data Processors and Data Custodians – These persons are responsible for the use, safe custody, transport and storage of data pertaining to the Council and its Clients.

2.3 Information Security Principles

The following principles provide a framework for the security and management of the Council's information and information systems.

a) Information should be classified in line with the Information Classification Framework and in accordance with any other legislative, regulatory or contractual requirements that might increase the sensitivity of the information and security requirements.
b) The Data Protection Officer is responsible for ensuring that data is classified and that in partnership with Data Custodians the information is treated in line with its classification level with appropriate procedures and systems in place to cater for this. Where personal data are stored, appropriate consent for storage and processing must be gathered and recorded as defined in the General Data Protection Regulation EU (GDPR) 2016/679, in force from the 25th May 2018.
c) All individuals covered by the scope of this policy must handle information appropriately in accordance with its classification level.
d) Information should be only available to those with a legitimate need for access.
e) Information will be protected against unauthorised access and processing.

f) Information will be protected against loss and corruption.
g) Information will be disposed of securely and in a timely manner with measures appropriate for its classification.
h) Breaches of policy must be reported to the Data Protection Officer and Clerk by anyone aware of the breach as soon as it is practicably possible to do so.

2.4. Legal and regulatory obligations

The Council's staff and third parties must adhere to all current UK and EU legislation as well as regulatory and contractual requirements. A summary of the relevant legislation is included in the Council. Guide to legislation relevant to the Information Systems Security Policy.

2.5 Information Classification

The following provides a summary of the Information Classification levels which are part of the Information Security Principles.

Category - Highly Restricted

Description

Highly confidential information whose inappropriate disclosure would be likely to cause serious damage or distress to individuals and/or constitute unfair/unlawful processing of "sensitive personal data" under the Data Protection Act; and/or

Seriously damage the Council's interests and reputation; and/or significantly threaten the security/safety of the Council's staff and third parties.

Examples

- Sensitive personal data relating to identifiable living individuals
- Individual's bank details
- Large aggregates (>1000 records) of personal data such as personal contact details
- Non-public information that facilitates protection of individuals' safety or security of key functions and assets e.g. network passwords and access codes for higher risk areas

Category - Restricted

Description

Confidential information whose inappropriate disclosure would be likely to cause a negative impact on individuals and/or constitute unfair/unlawful processing of "personal data" under the Data Protection Act; and/or damage the Council's commercial interests, and/or have a negative impact on the Council's reputation.

Examples

- Personal data relating to identifiable living individuals
- Staff or Client contact details
- Audit data containing detailed financial information
- Audit data relating to ongoing commercial tender processes, valuations
- Audit data relating to payroll or staffing matters

Category - Internal Use

Description

Information not considered being public which should be shared only internally but would not cause substantive damage to the Council or other individuals if disclosed.

Examples

- Non-confidential internal correspondence e.g. routine administration such as meeting bookings and catering arrangements
- Meeting minutes, internal policies and procedures

2.6 Compliance and Incident notification

It is vital that all users of information systems at the Council comply with the information security policy. Any breach of information security is a serious matter and could lead to the possible loss of confidentiality, integrity or availability of personal or other confidential data. Such a loss may result in criminal or civil action against the Council including the loss of business and financial penalties.

Any actual or suspected breach of this policy must be notified to the Clerk and Data Protection Officer at the earliest possible opportunity. All security incidents will be investigated, and consequent actions may follow in line with this policy; the Council's disciplinary policy; and relevant laws.

The Data Protection Officer will be informed of any breach found to affect personal data in keeping with the Council's Data Protection Policy. Compliance with this policy shall form part of any contract with a third party that may involve access to the Council's systems or data.

3. Responsibilities

3.1 Individuals

Individuals must adhere to the Acceptable Use Policy and follow relevant supporting procedures and guidance. An individual should only access systems and information they have a legitimate

right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data. In particular individuals should adhere to the information security 'dos and don'ts' outlined in the table below:

DO	DO NOT
Do use a strong password of at least eight digits containing alpha and numeric characters and at least one capital letter. You must change it if you think it may have been compromised, or if a security alert is issued by a software or service provider to do so.	Don't give your password to anyone
Do report any loss or suspected loss of data immediately to the Data Protection Officer at: clerk@llantrisant-cc.gov.wales	Don't reuse your previous password(s) for any other account
Do be on your guard for fake emails from organisations that appear to be legitimate, i.e. Town Councils demanding you open a .PDF file or click on a link. Remember, always check the email address. Also screen phone calls requesting confidential information - report anything suspicious to the Data Protection Officer at clerk@llantrisant-cc.gov.wales	Don't open suspicious documents or links
Do keep software up to date and use an auto-updating antivirus on all possible devices	Don't undermine the security of the Council's systems
Do be mindful of risks using public Wifi or computers	Don't access the Council's Data Store, or systems using public Wifi
Do ensure the Council's data is stored on the Council's Data Store.	Don't copy confidential the Council's data without permission
Do password protect your personally owned devices, preferably with thumb print access if available. Always lock your device if you are to leave it unattended on a client site.	Don't leave your computers or phones unlocked when unattended

3.2 The Data Protection Officer

The responsibilities of the Data Protection Officer

The Data Protection Officer is responsible for the maintenance, security and proper usage of all data held by the Council, and for ensuring that data custodians who maintain and process Client data as part of their Auditing duties are aware of any additional requirements that are required to safeguard data above and beyond those for normal internal data.

The Data Protection Officer is also responsible for information security training, the publication of the Information Handling protocols, policy and compliance associated with the Data Protection Act and the General Data Protection Regulation EU 2016/679.

3.3 Data Custodians

Data custodians are responsible for the data stored on mobile information systems and smart devices that hold both the Council's own and Client data that is examined, processed, reported on and stored as a result of the Audit function. In addition to their individual responsibilities 3.1 they must:

- Ensure that the physical and network security of their system is maintained.
- Ensure that the system(s) they maintain is/are suitably configured.
- Ensure that all data is appropriately stored and backed up.
- Ensure that appropriate access controls are in place to meet the Legal requirements and those of the Data Protection Officer.
- Understand and document any data security risk of which they become aware, take suitable steps to mitigate and ensure that this is communicated to the Data Protection Officer.
- Ensure that their systems are compliant with legal and the Council's contractual requirements.

3.4 IT Security Management

The Clerk is responsible for the Electronic Information Systems Security Policy and will, from time to time, advise on appropriate security measures for any new types of information systems that are introduced in order to aid clarity of the policy.

3.5 Computing Services

the Council will ensure the provision of IT infrastructure consistent with the demands of this policy and to support the Data Protection Officer, Data Custodians and Data Processors.

3.6 Internal Data Audit

The Council will conduct an annual Internal Data Audit across its digital estate to ensure, as far as it is reasonably possible to do so, that all Staff, Contractors, Sub-Contractors and Consultants abide by the Company's policies and that the Company is fully compliant with current Data Protection regulations and legislation.

4. Supporting regulations, policies and guidelines

Other policies issued by the Council support and reinforce this policy statement. These include but are not limited to:

- Data Protection Policy & General Data Protection Regulation
- Information Classification Framework and handling protocol
- User accounts Policy
- Acceptable Use Policy

Policy review

the Council will review this policy when required to ensure that it remains appropriate and up to date. Any questions or concerns should be made to the Data Protection Officer clerk@llantrisant-cc.gov.wales

5. Supporting documents

Guide to legislation relevant to the Information Systems Security

Mobile and Remote Working Policy

Data Custodian Policy

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version Number	V 1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

Document and Data Retention Policy

How Llantrisant Community Council responsibly safeguards Client data in electronic and paper formats ensuring that it is appropriately categorised, stored and erased for the purposes of Data Protection.

1. Introduction
1.1 Purpose

Information is one of the Council's corporate assets; in the course of carrying out its auditing functions, the Council accumulates information from both individuals and external organisations. the Council also generates a wide range of data, which is recorded in documents and records.

a) These documents and records are in several different formats, examples of which include, (but are not limited to) communications such as letters, emails and attendance notes; financial information including invoices, statements and reports; legal documents such as contracts, deeds, loan and finance agreements; and information relating to various types of financial transactions, including bank statements, investment statements, asset registers, tax records, payroll information and insurance policies.

b) For the purposes of this Policy, the terms 'document' and 'records' include information in both hard copy and electronic form.

c) In certain circumstances it will be necessary to retain specific documents in order to fulfil statutory or regulatory requirements as auditors and also to meet operational needs. Document retention may also be useful to evidence audit findings in the case of anomalies being identified, and also to preserve information which has evidential value.

d) Premature destruction of documents could result in inability to defend litigious claims, operational difficulties and failure to comply with the Freedom of Information Act 2000 and the General Data Protection Regulation EU 2016/679.

e) The retention of all documents and records is impractical. Disposal assists the Council to maintain sufficient electronic and office storage space and will de-clutter office accommodation, resulting in a more desirable working environment. It also ensures that the Council complies with the General Data Protection Regulation EU 2016/679.

f) It is important for the above reasons that the Council has in place systems for the timely and secure disposal of documents and records that are no longer required for business or statutory purposes.

2. Aims and Objectives

a) The key objective of this Policy is to provide the Council with a simple framework which will govern decisions on whether a particular document should be retained or disposed of. In the

case of documents which are to be retained by the Council, the Policy includes guidance on the format in which they should be retained and appropriate retention periods.

b) Implementation of the Policy should save the Council's officers time when retrieving information, in particular by reducing the amount of information that may be held unnecessarily.

c) The Policy clarifies the different roles of the Council officers in relation to document retention and disposal in order that they understand their responsibilities, and who to refer to if they are unsure about any document and require clarification.

d) It is envisaged that this Policy will assist the Council in securing compliance with legal and regulatory requirements, including the Freedom of Information Act 2000, the Environmental Information Regulations 2005, the General Data Protection Regulation EU 2016/679 and the Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. In addition to assisting officers in their day to day business, this should also ensure that searches for information requested under the Freedom of Information legislation are as quick as possible.

e) Additionally, the Policy should help to ensure that the Council archives records and documents that are of historical value appropriately for the benefit of future generations.

3. Scope

a) This Document Retention Policy applies to all information held by the Council and any external service providers in the event that such an organisation is processing information on the Council's behalf.

4. Policy Statement

a) the Council will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it requires to carry out its' statutory functions and the provision of its auditing services.

5. Retention and Disposal Policy

a) Decisions relating to the retention and disposal of documentation should be taken in accordance with this Policy, in particular:-

- Appendix 1 – Disposal and Retention Considerations – a checklist to be followed where the disposal of any document is being considered.

- Appendix 2 – Document Retention Schedules – Comprehensive guidance on the recommended and statutory minimum retention periods for specific types of documents and records.

b) In circumstances where a retention period of a specific document has expired, a review should always be carried out prior to a decision being made to dispose of it. This review should not be particularly time consuming and should be straightforward. If the decision to dispose of a document is taken, then that document will be disposed of securely by shredding and subsequent destruction in relation to paper documents or deleted from electronic storage using a permanent delete application.

6. Roles and Responsibilities

a) The Clerk will be responsible for determining (in accordance with this Policy) whether to retain or dispose of specific documents within the remit of their service area.

b) The Clerk may delegate the operational aspect of this function to the Data Protection Officer.

c) The Data Protection Officer should seek legal advice if they are uncertain as to whether minimum retention periods are prescribed by law, or whether the retention of a document is necessary to protect the Council's position where a potential evidentiary issue has been identified.

d) The Data Protection Officer should ensure that the Schedule in Appendix 2 which is relevant to the Council's services is kept up to date.

7. Disposal

a) Confidential waste documents should be made available for collection by use of the confidential waste sacks which are provided to consultants by the Council in order that they can be destroyed. It is essential that any documents which are to be thrown away and contain confidential or personal data must be disposed of in this way, in order to avoid breaches of confidence or of the General Data Protection Regulation EU 2016/679.

b) Disposal of documents other than those containing confidential or personal data may be disposed of by binning, recycling, and permanent deletion (in the case of electronic documents), and the transfer of documents to external bodies. Transfer of documents to external bodies will be unusual but could be relevant where documents are of evidentiary interest and may therefore be sent to the investigating authority, i.e. the Police or HMRC.

c) Records of disposal should be maintained by the Data Protection Officer, and should detail the document disposed of, the date and the Consultant who provided the document for disposal.

APPENDIX 1
Disposal and Retention Considerations

Each of the following questions and guidance underneath them should be considered prior to the disposal of any document.

1. **Has the document been appraised?**

   - Check that the nature and contents of the document is suitable for disposal.

2. **Is retention required to fulfil statutory obligations or other investigatory obligations?**

   - Specific legislation setting out mandatory retention periods for documentation held by local government is very limited, but includes the following:-

     - Tax legislation – minimum retention periods for certain financial information are stipulated by the VAT Act 1994 and the Taxes Management Act 1970.
     - The Audit Commission Act 1998 – Provides auditors with a right of access to every document relating to a Council Audit that appears necessary for the purposes of carrying out the Council's function under the Act.
     - The Local Government Act 1972, Part VA – Governs public access to certain documents relating to Council's minutes and the management of Committee meetings.

3. **Is retention required for evidence?**

   - Keep any documents which may be required for legal proceedings until the threat of proceedings has passed.
   - The limitation period for commencing litigation should also be a key consideration. This is governed by the Limitation Act 1980 and the main time limits that apply directly to local government are:-

     - Contract or tort (such as negligence or nuisance) claims (other than personal injury) cannot be brought after six years from the date on which the cause of the action occurred.
     - Personal injury claims cannot be brought after three years from the date on which the cause of action occurred.
     - Claims based on provisions contained in documents that are 'under seal' cannot be brought after twelve years from the date on which the cause of action occurred.

   - There is no statute of limitation for a criminal offence. Any document deemed to be evidentiary in nature in result of a criminal offence will be passed to the relevant investigating authority and a copy retained until the conclusion of the investigation.

Appendix 2
Document Retention Schedules

1. Introduction

The following schedules provide guidance on the retention periods applicable to a wide range of the Council's Internal Audit Documents and supporting evidential documents copied from the Audit subject. Copies may be retained electronically or in hard copy on the proviso that electronic copies of all documents should be acquired for retention where it is possible for the Auditor to do so.

2. Explanation of Retention Schedule Headings

a) There is a Document Retention Schedule for each document type. The headings in each Schedule are as follows:

b) **Reference Number** – This section provides ease of reference.

c) **Function Description** – The Schedule provides notes that define each function in terms of related activities.

d) **Retention Action** – This entry provides the guidance as to whether the document should be retained, and if so how long for. It also provides guidance regarding the method by which documents should eventually be disposed of.

e) **Examples of Records** – This section provides common examples of the type of records included within the particular function. This list is not exhaustive.

f) **Notes** – This indicates if the retention action is common practice or statutory.

3. Glossary of Terms

Archiving – The method of archiving selected may include, but will not be limited to, electronic storage on records management systems, storage in secure filing cabinets, strong rooms or other designated areas within the Council's offices.

Administrative Use – When business use has been ended or the file has been closed.

Closure – 'Destroy 'x' years from closure'. A record/file is closed when it ceases to be active. After closure, no new papers/information should be added to the record. Triggers for closure of a file include: reaching an unmanageable size; covering a period of 'x' years or more; no records added for 'x' period of time; no action taken after 'x' period of time.

Closure Period – Specified period of time during which the record is subject to restrictions on provision of access to staff and/or the public may be dictated by statutory requirements or by the authority's policy. Any closure period should comply with current legislation on access to local government information – including the General Data Protection Regulation EU 2016/679 and the Freedom of Information Act 2000.

Common Practice – Standard practice followed by the Council and by those local authority records managers who are members of the Records Management Society.

Last Action – 'Destroy 'x' years after last action.' Date of most recent amendment / addition / deletion of information.

Permanent – Records which must be kept indefinitely for legal and/or administrative purposes, and/or are of enduring value for audit trail purposes and so suitable for transfer to the Council's archive.

Page 47 of 74

Data Retention Schedule – Client Audit				
Ref No.	**Function Description**	**Examples of Records**	**Retention Action**	**Notes**
INTERNAL AUDIT				
IA1	**Cashbook**	**Review**	**Retain**	
	The process of making substantiated and structured observations in each area of the annual Internal Audit process	**PERMANENT** • Findings of audit testing in each area of Internal Audit Review are recorded in Internal form the Council IA Programme for the corresponding financial year	• Auditors observations substantiated by information contained within the council's accounts system and supporting documentation	Common practice
ACCOUNTING RECORDS				
AR1	**Cashbook**	**Review**	**Retain**	
	The process of examining the method by which councils maintain their accounting records.	• Cashbook records for the audit period. • Cost Centre and Coding schedule. • Copy of current Year opening Trial Balance. • Copy of Prior Year external audit report *NB: copies of intermediary Trial Balances, journals, etc., shall not be retained unless any significant reportable issues are identified*	• Copy of Cashbook(s) • Copy of external audit certificate and report	Destroy after 10 years
GOVERNANCE & ACCOUNTABILITY				
GA1	The process of examining the conduct and operation of councils in relation to the proper uses of statutory powers and delegated authorities.	• Review of minutes to be completed using Internal form the Council Review of Minutes • Current Standing Orders and Financial regulations	• Anonymised extracts from Council minutes in the Annual Minute Review recorded in the Council Review of Minutes.	Destroy after 24 months

Page 48 of 74

		• Financial procedures obtained in electronic format • the Council Internal form	• the Council	
Payments and VAT				
PV1	**Payments testing**	**Review**	**Retain**	
	The process of examining the authenticity and accuracy of payments made by the council.	• Payment testing schedule (electronic format only): Internal form the Council	• Tender registration number on contractsfinder.gov.uk • the Council	Destroy after 10 years
Risk Assessments & Insurance Schedules				
RAI1	**Risk Assessments**	**Review**	**Retain**	
	The process of examining councils' Financial and Health & Safety Risk Management procedures.	• Financial and Health & Safety Risk Assessments	• LCRS or other Risk Register • Health & Safety Risk Register • Playground Risk Management Policy	Destroy after 10 years
RAI2	The process of examining council's Insurance policies and schedules.	• Insurance schedule for the Financial Year being audited	• Insurance policy/policies • Insurance schedule(s)	Destroy after 10 years
Budgetary Control & Reserves				
BCR1	**Budget setting and analysis of reserves**	**Review**	**Retain**	
	The process of examining the Budget setting process and the testing of councils' reserve funds.	• Year-end budget outturn report • Annual fund reserve analysis including movement testing	• Outturn report with headline data and comment • Schedule of Reserves detailing year on year movement	Common Practice
Review of Sources of Income				
RI1	**Income testing**	**Review**	**Retain**	

Page 49 of 74

	The process of examining councils' sources of income, ensuring that said income is collected and recorded appropriately and that fees and charges are being correctly reviewed, set and billed.	• Current years fees • Procedural notes on income stream(s) • Outstanding debt • Nominal ledger balances	• Published fees • Nominal ledger income reports • Schedule of outstanding debts	Destroy after 24 months
RI2	**Income Analysis**	**Permanent** • Copies of anonymised income streams with all personal details redacted: Internal Form the Council • Internal Form the Council	• the Council Internal forms	Common practice
Petty Cash & Bank Cards				
PCB1	**Ad hoc expenditure**	**Review**	**Retain**	
	The process of examining the authenticity and accuracy of councils' cash and credit / debit card payments.	• Copy of sample petty cash reclaim indicating balance at time of visit to be agreed to the physical cash holding. • Detail of petty cash holding • Detail of cash floats (bars, tills etc) • Detail of procedural documents for use and settlement of credit / debit cards.	• Petty Cash statement • Cash float statement	Destroy after 10 years
Staff Salaries and Wages				
SSW1	**Payroll analysis**	**Review**	**Retain**	
	The process of examining the authenticity and accuracy of Salary, Wage and Agency payments made by or for and on behalf of the council.	• Schedule identifying staff name, post held, SCP scale point or approved annual salary and basic weekly hours • Variable pay documents • Salary payment summary for month examined • HMRC and Pensions submission for month examined	• Internal form the Council	Destroy after 24 months

Page 50 of 74

Asset Registers				
AR1	**Asset Register(s)**	**Review**	**Retain**	
	The process of examining the authenticity and accuracy of Council's Asset Register(s)	**PERMANENT** • Asset Register containing headline detail of acquisitions and disposals to be reconciled to the previous year's Asset register.	• Asset Register	Destroy after 24 months
Investments and Loans				
IL1	**Investments**			
	The process of examining the authenticity and accuracy of Councils' investments, ensuring that the returns are being received and accurately recorded.	**PERMANENT** • Schedule of investments held at the Financial Year-End • Investment strategy	• Investment statements confirming YE position only • Investment strategy/policy	Common practice
IL2	The process of examining the status of Loans obtained or let by Council's.	**PERMANENT** • Examination of Loans approved or acquired in the Financial Year under examination. • Examination of year-end liability/exposure • Signed loan agreements where the council has issued a loan	• Loan Application & confirmation of draw down • Year End balance statements (Loans acquired / issued)	Common Practice
Bank Reconciliations				
BR1	**Bank Reconciliations**			
	The process of examining and verifying the accuracy of the accounting records held by Council's and the agreement of Opening and Year End balances.	• Reconciliations, by account, for each bank / building society held • Associated finance organisation statements for Year End date • Bank Statement for each Bank Account as at the 31st March in the year being audited	• Internal Form the Council 11.2 Bank Reconciliations.	Destroy after 24 months

Statement of Accounts / Annual Return				
SAAR1	Year End statutory information			
	The process of examining the authenticity and accuracy of Councils' Annual Accounts ensuring that the publish accounts are accurate to the fullest extent possible.	**PERMANENT** • AR Statement of Accounts for year being audited • Detailed Accounting statements • Year End Accruals • Stock Check reports • Year End Trial Balance • Headline finance information in Internal form the Council • Internal Form the Council Annual Return Data	• Formal Statement of Accounts (where prepared) • Balance Sheet: I&E or R&P accounts • Debtors & Creditors YE reports • Stock Check reports • Year End Trial Balance	Common practice

Page 51 of 74

Appendix 3

E-mail Retention Guidance

1. Introduction

To ensure fair Processing, E-mails will not be retained by the Council for longer than necessary in relation to the purposes for which it was originally retained.

The length of time for which the Council is required to retain E-mails is set out in the 'Data Retention Schedule – Client Audit' above. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All E-mails shall be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain them.

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version number	V1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

Page 52 of 74

Information Classification Framework

How Llantrisant Community Council categorises information and holds it according to sensitivity and confidentiality.

Introduction

This document outlines The Council's implementation of a holistic system of categorising the information it holds according to *sensitivity* and *confidentiality*. The framework also defines associated rules for the handling of each category of information in order to ensure that the appropriate level of security is implemented and maintained.

The Information Classification Framework aims to facilitate compliance with the requirements of The Council's Data Protection and IT Systems Security Policies, particularly in relation to cyber security.

Scope

All information held by or on behalf of The Council, in any form including digital, paper or any other media is subject to the requirements of this framework. Information handling rules apply to all The Council's staff and third parties handling The Council information and client information that may be held by The Council.

Requirements

Information shall be categorised according to the *Information Classification Scheme*. The categorisation shall be determined by the originator or designated owner of the information and all information falling into the 'restricted' or 'highly restricted' categories shall be appropriately treated as such.

Information shall be handled in accordance with the Information Handling Protocol. Where particular information falls into more than one classification category, the higher level of protection shall apply in that instance.

Where a third party will be responsible for handling information on behalf of The Council, the third party shall undertake to adhere to these data handling requirements prior to the sharing of that information. This is of the utmost importance when 'personal data' or 'sensitive personal data' as defined by the Data Protection Act and General Data Protection Regulation is concerned.

Where The Council holds information on behalf of a Customer for the purposes of conducting an internal audit under The Audit Commission Act 1998 that information shall be stored in an anonymised format and under its own information classification system.

Responsibilities

It is the responsibility of all individuals to categorise and handle information appropriately according to this framework. Failure to do so may be considered a breach of The Council's Data Protection and or IT Systems Security Policies and could result in disciplinary action.

The Council shall ensure that the Information Classification and Handling Framework documents are reviewed regularly to ensure they remain fit for purpose.

Policies

- Data Protection Policy
- IT Systems Security Policy
- Information Handling Protocol

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version Number	V1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

Information Handling protocol

Llantrisant Community Council's protocol for the safe and secure handling of information in paper or electronic format.

Page 55 of 74

Introduction

As responsible Data Controllers we must demonstrate that we properly control and restrict access to data to the people who have the correct authority to allow them to use it.

Location/format of information	Highly restricted	Restricted	Internal use
Shared file storage areas on The Council's data storage facility	• Strictly restricted access on a need to know basis.	• Limit number of, and identify, individuals who have access to folders.	• No internal restrictions
Sending email from The Council hosted account to an external account	• Double check recipient(s) are correct. Auto-forwarding to external account should be avoided. • Consider secure alternatives to using email • Consider password encryption of file with strong password: At lease eight alpha numeric characters including capital letter(s)	• Check recipient(s) are correct. • Auto-forwarding to external account should be avoided	• Check recipient(s) are correct.

Sending email from externally provided personal account: e.g. yahoo.	• Avoid: Please be aware that any data in sent items or your inbox will be stored outside of The Council secure systems.	• Avoid: Please be aware that any data in sent items or your inbox will be stored outside of The Council secure systems.	• Use organisational email accounts wherever possible
Paper copies	• Must be stored in secure environment • e.g. locked cabinet/drawer. Must not be left unattended in an insecure environment. • Must be disposed of securely (e.g. confidential shredder).	• Should be stored in secure environment e.g. locked cabinet/drawer. • Should not be left unattended in an insecure environment. • Should be disposed of securely (e.g. confidential shredder).	• No restrictions
Postal service	• All information must be sent in a sealed and taped envelope and marked 'highly restricted' clearly addressed and containing the sender's details. • Must be sent via tracked and signed for mail.	• Sealed envelope marked 'restricted' with sender details. • Must be sent via tracked mail.	• No restrictions
Fax machine	• Only use if recipient has verified security of receiving machine and is at machine awaiting receipt. • Double check number. • Use cover sheet.	• Only use if recipient has verified security of receiving machine.	• No restrictions

1) Where it is not possible to implement the above protocols, consider whether the restricted information can be **redacted** or **anonymised**. If this is not possible, appropriate security measures should be implemented (for example agents on mobile devices containing personal data and appropriate physical security measures for paper records).
2) Any potential loss or unauthorised disclosure of **personal data** and or **sensitive personal data** must be reported The Council's Data Protection Officer clerk@llantrisant-cc.gov.wales as soon as practicably possible.

Page 56 of 74

Mobile Computing Policy

How to responsibly use mobile phones, tablets and other digital devices to protect data on devices owned by you or Llantrisant Community Council.

1. Introduction

1.1 Purpose

There is a developing business need for increasing numbers of colleagues to use mobile computing devices to conduct Auditing activities remotely from Client offices, and at Llantrisant Community Council remote offices.

The purpose of this policy is to outline The Council's requirements of mobile computing users in relation to the proper stewardship of mobile computing assets and the security of information accessed whilst using such devices.

This policy is part of a set of The Council's documentation covering information security and it should be read in conjunction with the:

- Data protection policy
- Data management protocol
- IT security policy
- IT acceptable use policy
- Audit data policy

The aspects of this policy relating to stewardship of The Council's mobile computing assets. The information security aspects of this policy apply to all mobile computing devices, both owned by The Council and third-party owned devices, used to access The Council's systems and services remotely and on a stand-alone basis.

1.3 Definition

For the purpose of this policy, "mobile computing devices" refer to all forms of portable computing equipment that can store digital data. Examples include, but are not limited to, laptops, netbooks, tablets and mobile phones.

1.4 Roles and Responsibilities

The Clerk is responsible for approving and regularly reviewing The Council's policies which contribute to the set of documentation covering information technology and security. The Data Protection Officer is responsible for developing awareness and guidance in the area of information security and for advising the Clerk and individual users on the use of mobile

computing to meet business needs and the most appropriate technical responses to maintaining information security.

Users of mobile computing devices are responsible for ensuring that such devices are purchased, used and disposed of in accordance with The Council's policies and procedures. In particular, users must ensure that they act in accordance with The Council's various information security policies and that they have completed the Company's mandatory training on information security and update training held during The Council's bi-annual Team meeting.

2. Policy

2.1 Stewardship of Mobile Computing Devices

All equipment purchased by The Council, including mobile computing devices purchased by the Company remain the property of The Council. They must be returned to the Company on request or on termination of employment.

Mobile computing devices should be used for the intended business need and in accordance with The Council, information security and acceptable use policies, i.e. mobile devices should be used only by The Council's staff for company related business. Incidental personal use, allowable by HMRC, where it is consistent with any requirements of The Council's IT policies.

The security of any institutional data stored on a mobile computing device must be given due consideration. Any unique data generated on such a device should be copied onto The Council's data store at the earliest opportunity and interim backups stored on a secure remote hard drive, USB key or other appropriate device.

Users with Accounts Software packages licenced to The Council on laptops must ensure that the software, loaded onto the machine is used in compliance with the appropriate license(s) and copyright considerations. If in any doubt, the Data Protection Officer should be consulted.

Users are responsible for maintaining the currency of the computer operating systems, antimalware and productivity applications ("patching"). Either automated (recommended) or manual method may be used. It is not permitted to make any alterations to the hardware or software that significantly impair security. If the user is not comfortable patching their device, they should return it to their IT supporter on a regular basis, allowing sufficient time for updates to be installed.

If a user has any reason to suspect that their device has become infected with malware, they should immediately cease to use it, and take all necessary steps to conduct a thorough examination of the device and appropriate disinfection of the device as required.

Users should seek advice from the Data Protection Officer before passing on, discarding, or otherwise disposing of, any mobile computing device to ensure that all data pertaining to The Council and its Clients has been permanently deleted.

2.2 Information Security

All users of mobile computing devices which access The Council digital data must complete The Council mandatory training unit on information security. Training updates are given to all staff and consultants annually, at the Annual Team Meeting, and via update reports from time to time as required.

Users are responsible for the physical security of their mobile computing devices and any The Council, or The Council's Client's data stored on it.

Information being accessed or processed using mobile computing devices should be treated in accordance with The Council's Data Management Protocol. Any loss of mobile computing device or suspected breach of information security should be reported immediately to the Clerk. Suspected theft of a mobile computing device should also be reported to police at the earliest opportunity.

Users should avoid internet café and other public wi-fi connections as these pose information security risks and should be avoided especially when accessing highly sensitive information.

Users of private devices are responsible for ensuring that they maintain anti-virus software, operating systems and security updates, as appropriate to the equipment, if they use it to access, store or process The Council's Client's digital data.
Computing Services may monitor and log network and e-mail usage as a means to protect information.

3. Breach of the policy

3.1 If a staff member or consultant is found to have acted in breach of this policy, this may lead to disciplinary action being taken against them. This disciplinary action could be up to and including dismissal.

Document Control Information

Owner	Llantrisant Community Council
Version number	V1.0
Original approval date	10th December 2024
Approved by	Llantrisant Community Council
Date of last review	10th December 2024
Date of next review	2028

LLANTRISANT COMMUNITY COUNCIL
Data Protection Act 1998
Subject Access Request Form

1. Personal Details of Subject

Title	Forename(s)	Surname
Any previous name known to Llantrisant Community Council		
Date of birth	Current telephone number	
Current Address	Current email address	
Relationship to the Council	Start and end dates of employment, contract or Client relationship with the Council.	
Staff ID number or Client reference		
Any other information that could help identify your personal data		

2. Alternative Contact Details (third parties only)

Only complete this section if you are **not** the data subject, e.g. you are requesting information relating to another person.

Title	Forename(s)	Surname
Address	Telephone number	
	Email address	
Relationship to data subject		

3. Records Required

(PLEASE COMPLETE ALL SECTIONS)

A. Please tick the category into which your enquiry falls

Category	✓
Council data records	
Disciplinary records	
Grievance records	
Other HR related documents	
Health and medical matters	
Political, religious or trade union information	
Personal details, e.g. name, address and date of birth	
Other (please specify or describe if possible)	

B. Please describe the information you seek <u>in as much detail as possible</u>. This will help us to identify the information you require. For example, 'Information relating to me contained in the April 2024 Minutes of the Full Community Council …' or 'emails about me relating to x matter sent by A.N. Other between the 31st March and the 30th April 2024.

C. Sections / Departments to search

Please tick below which (if any) of the following sections/departments the documents you are seeking may be found or which you would like us to search.

Section / Department	Search (✓)
Your Council	
Human Resources	
Payroll	
Finance Office	
Council Services	
• Invoice information	

• Market Stall information	
• Allotment register	
• Lease information	
• Council Services information	
Other (please specify if possible)	

4. <u>Identity</u>

If you are requesting personal data of which you are the subject you must supply:

(a) a notarised photocopy of proof of identity with this form, such as passport, driving licence or Military ID card, and,

(We do not make this charge to current members of staff or current clients).

If you are requesting personal data on behalf of a subject you must describe your relationship to the subject and supply:

(a) written signed authority of the subject;

(b) a notarised photocopy of proof of the subject's identity with this form, such as passport, driving licence or Military ID card; and,

5. <u>Declaration</u>

I certify the information provided in this form is accurate to the best of my knowledge. I accept that the Council will take reasonable steps to establish identity prior to release of personal data.

I request that the Council provide me with a copy of personal data relating to the subject named in Section 2 of this form.

I enclose the following:

☐ A photocopy of the data subject's proof of identity;

☐ Written and signed authority of the data subject (third parties only).

Signed	Please print name	Date

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version number	V1.0
Original approval date	10TH DECEMBER 2024
Approved by	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

User Account Policy

Eligibility for and the use of Llantrisant Community Council user accounts

Introduction

Effective management of user accounts is vital to ensure that correct access rights are granted to the Council information systems and that this access is restricted to authorised users only.

Scope

This policy covers all information systems used to conduct the Council Auditing business and those which are connected to the the Council network.

Requirements

Access to computing facilities is via individual username and password which allows access to login to the Council Data drives; make use of private file space, run software, access and use email facilities, share and transfer files.

Accounts are issued for individual use only. For security purposes, users may not share, loan or give away account or password information to any other person. User accounts are to be used only by the assigned user of the account for authorised purposes. Passwords should not be shared, emailed or published. Default passwords should be changed as soon as practically possible and in no more than 48 hours.

Attempting to obtain another user's account password is strictly prohibited. Users are required to change their password if they have reason to believe their account has been compromised in any way. Users are required to take all necessary precautions to prevent unauthorized access to the Council computing resources. Should a business need require the sharing of data with a third party, the request must be passed to the Data Protection Officer for approval.

Users must be aware of and understand the Acceptable Use Policy before accepting and using an account.

Eligibility

There are two categories of people who are eligible for access to computing facilities:

- All staff who are employees of the the Council
- Third parties who provide consultancy services to the Council

Third parties must be real individuals. Accounts are not issued to groups, committees, services or similar. In normal circumstances they will be consultant Auditors who provide auditing services for and on behalf of the Council, but they could be anyone the management team considers in need of computing facilities for the Council work.
the Council takes full responsibility for third party and staff records and the computer usage of those concerned. the Council must remove the records when the third parties leave or no longer requires computing facilities. The maximum time that a record can exist before review is 24 months.

Accounts and password management

All staff and third parties will receive computer accounts upon entering into either an employment or service contract with the Council and a username and initial password will be assigned.

New staff or third parties may be informed of an initial temporary password communicated via a secure channel which shall be valid for a limited time period only. Temporary Accounts shall not be issued.

User accounts are subject to closure in the following circumstances:

- Staff or third parties leaving the the Council - the account is closed on or shortly after the last day of employment.
- Dismissal of staff or third parties where the account is closed immediately. Following the closure, stored data associated with the account can be released with appropriate liaison with the Clerk and/or Data Protection Officer (under normal legal safeguards) if appropriate or required.
- Dismissal of staff or third parties where external agencies, in particular the police, are involved - the account is frozen immediately and access disabled.
- Sudden death not requiring investigation - the account is disabled immediately.
- Death involving a subsequent investigation - the account is frozen, and access disabled immediately. Frozen accounts are maintained for as long as is required by any investigations.

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version number	V1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

Data Processor and Data Custodian policy

How Llantrisant Community Council acts as a responsible Data Controller, protecting company and client data on company owned and private computing devices

1. Introduction

1.1 Purpose

Staff and Consultants have access rights to confidential client information at Llantrisant Community Council, the Data Controller. The role of these personnel within the Information Systems Security policy is defined as Data Custodians and they are responsible for the safe custody, transport, storage of the data. the Council expects that all staff and third parties will exercise the highest ethical professional conduct, at all times, and exercise a duty of care to all clients which originate the data that they maintain. This document sets out the responsibilities and required behaviour of staff who maintain client information at the Council.

Scope

Information systems at the Council shall be managed by suitably skilled staff to ensure their continued security. This policy covers all personnel who have elevated privileges on any computer system which is used to access the Council's systems, licenced software and client data, and also covers Data Custodians with access to and responsibility for maintaining client data.

Guidelines

Data custodians are key to ensuring the security of the Council's information systems. The high-level requirements for Data Custodians are defined in the information Systems Security policy and form the basis for the additional guidance given here. Data custodians must:

Ensure that physical and network security is maintained

Data Custodians should ensure the physical security of their computers, laptops, tablets and smart devices by taking measures to restrict and monitor the physical access to them. These devices should not be left unattended on public transport, or in parked motor vehicles. When remote working on Client Site, devices should always be locked when left unattended.

Network access to the Council servers should be limited to only those that require access. Remote access to administrative services should be assessed separately and have additional restrictions where possible. Regular network vulnerability assessments will be made on live systems and the results published to system owners.

Ensure systems are suitably configured, maintained and developed

Data Custodians should maintain protected systems to agreed secure baselines based on industry best practice:

All systems must be password protected, installed with an approved data security and anti-virus package that is permanently active on the system.

Data Custodians must apply software patches in a timely manner to address published vulnerabilities or those highlighted through automatic scanning. High priority patches must be applied in accordance with supplier recommendations or within two weeks, whichever is shorter. Where this is not possible due to service commitments other compensating control measures should be taken to mitigate the risk and the risk reported to Information Systems Administrator.

Appropriate data back-up and storage

Backups of Client Data should be performed on a daily basis, to an external hard drive or similar, and to a physically separate location where possible. Data should be synchronised with the Council's main server on at least a weekly basis.

Commercial and free data cloud providers

Commercial and free cloud providers offer convenience and simplicity for services such as email and storage. However, there are risks to their use and it is important that these are understood so that sensible decisions can be made about the suitability of their use for any given purpose.

Unlike the use of private cloud drives, users of the free services must accept the provider's terms and conditions. the Council cannot ensure that confidentiality, integrity and availability of the information, or the location of the country in which the data is stored without a formal agreement in place. If there are legal or reputational consequences should the information you are storing be lost, stolen, or seen by unauthorised persons or organisations, you should not use a cloud service provider to store, transmit, or process it. The storage of personal data with such providers is likely to be a breach of the Data Protection Act and the General Data Protection Regulation for which the Council could be penalised by the Information Commissioner.

Ensure that appropriate access controls are in place to meet the requirements of the Data Protection Officer

Access to all systems must be made through a secure authentication process apart from read-only or publicly available information and only given to those who require access. Administrator accounts with elevated privileges should only be used to carry out specific tasks and not used as a matter of routine. The principle of least privilege should be applied at all times.

Data Custodians should record the classifications of the data held on their systems and the potential access routes to this data and the controls on them. These records should be used in a discussion with the Data Protection Officer to ensure that they meet the levels needed.

Understand & document risks, take suitable steps to mitigate and ensure that the Information systems administrator is advised

Data Custodians should understand the potential risks in the use of their systems while remote working. Significant concerns should be highlighted to the Data Protection Officer and placed in the Computing Services risk register and monitored.

Publish procedures for users of the systems to allow secure access and usage

The Information Systems manager and Data Protection Officer will ensure that sufficient documentation is made available to all users of the Council's systems to allow secure access and storage. This documentation shall be reviewed and updated so that it matches current security requirements as this change from time to time.

Ensure systems are compliant with legal & contractual requirements

Data Custodians should ensure that they have a full understanding of the legal and contractual requirements of the data and systems that they maintain when the service is used in accordance with the service description. They are authorised to act promptly to protect the security of their systems but any actions they take should be balanced and proportionate particularly when undertaking actions that would have a direct impact on the users of their or other systems. Actions that might potentially be invasive of a user's reasonable expectations of privacy must be undertaken in accordance with the guidelines on investigation of computer use.

Logging should be put in place to record the use and attempted use of information systems. The data logged should be sufficient to support the security, compliance and capacity planning requirements. Logging for normal user actions should not be unnecessarily intrusive whereas logs for system administrator access should record all actions. Logs should be recorded on a separate system to the one being monitored and secured to prevent unauthorised modification. Logs should be held for a defined period and then deleted automatically unless they been specifically identified as required for investigation.

The Data Protection Act requires that any personal data is collected for specific purposes and is deleted when it is no longer required.

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version Number	V1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

Legislation impacting Llantrisant Community Council's GDPR Policy

Legislation which governs the way in which Llantrisant Community Council, its Staff and third parties are required to acquire, manage, store, use and distribute data.

Introduction

This document contains guidance on some of the principal relevant legislation that is relevant to the information systems of Llantrisant Community Council. This legislation must be adhered to in order for The Council to remain legally compliant in the storage, processing or transmission of information.

UK Legislation

The Local Authority & Accountability Act 2014

The Local Audit and Accountability Act 2014, Regulation 5, provides auditors with a; **'right of access to all documents and files relating to a Council Audit that are considered necessary by those conducting the audit.'** It is not a requirement to seek the personal consent of the individuals whose personal data is contained within documents or data in order to gain access to these for Internal Audit Purposes.

Such documents and files include, but are not limited to, Accounting Systems back up files including cashbooks, financial reports and associated spreadsheets, payroll records and employment contracts. Additionally, records of services provided to clients of the council are also reviewed. These may include allotment lease records, burial and memorial records, market stall records, facilities booking receipts, invoices and other similar items.

Computer Misuse Act 1990

http://www.legislation.gov.uk/ukpga/1990/18/contents

http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990

The Computer Misuse Act is intended to deter criminals from using a computer to assist in the criminal offences or from impairing or hindering access to data stored in a computer. The three criminal offences defined in the act are:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

The Crown Prosecution Service offer further guidance in relation to the Computer Misuse Act.

Data Protection Act 1998

http://www.legislation.gov.uk/ukpga/1998/29/contents

1. Data protection act is underpinned by these guiding principles
2. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
3. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
4. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. Personal data shall be processed in accordance with the rights of data subjects under this Act.
8. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
9. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Freedom of Information Act 2000

http://www.legislation.gov.uk/ukpga/2000/36/contents

Page 69 of 74

The Freedom of Information Act 2000 promotes greater openness and accountability across the public sector and gives a general right of access to all types of recorded information held by public authorities, subject to exemptions applying. The Council., has an obligation to the public under the Freedom of Information (FOI) act; requests and responses are managed by the Freedom of Information Officer, based at The Council's head office. The act covers all recorded information held in documents, memos, emails and other written communications that are produced by any member of staff or consultant acting on behalf of the company. Almost any document we write at work could potentially be released. Do not write anything in an email that you would not be happy to see printed on The Council letterhead.

As an employee or a consultant, if you receive a non-routine request for information you should forward it immediately to the Freedom of Information Officer [1] by email to the contact address of clerk@llantrisant-cc.gov.wales. Please remember there is a twenty-working day legal deadline to respond to requests (starting from next working day after the request is received). A fee of £55 plus VAT is made in respect of every Freedom of Information request.

Regulation of Investigatory Powers Act (RIPA) 2000

http://www.legislation.gov.uk/ukpga/2000/23/contents

RIPA regulates the powers of public bodies to carry out surveillance, investigations, and covers the interception of communications. The Home Office offers guidance and codes of practice on its application and the circumstances that it should be used.

https://www.gov.uk/guidance/surveillance-and-counter-terrorism

A Draft Investigatory Powers bill is passing through parliament and will reform the requirements of RIPA.

Copyright, Designs and Patents Act (CDPA) 1988

http://www.legislation.gov.uk/ukpga/1988/48/contents

The act defines and regulates ownership of rights in intellectual property generally provides the owner with a right to prevent others using it unless they have permission or a licence. CDPA categorises the different types of work that are protected by copyright:

- Literary, dramatic and musical works;
- Artistic works includes buildings, photographs, engravings and craftsmanship.
- Sound recordings and films;

Page 70 of 74

- Cable programmes; published editions and broadcasts.

Counter-Terrorism and Security Act (CTSA) 2015

http://www.legislation.gov.uk/ukpga/2015/6/contents

CTSA has a number of measures and contains a duty on specified authorities including Higher Education to have due regard to the need to prevent people from being drawn into terrorism. This is also known as the Prevent duty.

Defamation Act 1996

http://www.legislation.gov.uk/ukpga/1996/31/contents

Defamation is speaking, broadcasting, printing or publishing something which might harm a person, company or institution's reputation. This includes not only the words themselves but also their implications. Personal digital archives may include opinions which another person could consider as libellous and by making such records available in a digital archive, whether online, or in a designated reading area, the digital archivist could be considered as 'publishing' that archive. Actions can be brought against individual members of staff as well as <<ORGANISATION>> itself.

Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/contents

The Human Rights Act 1998 allows an individual to assert the rights of the ECHR (European Convention on Human Rights) against public bodies in UK courts and tribunals. Article 8 ECHR provides:

- for the right to respect for private life, family life, one's home and correspondence, and
- that there shall be no interference by a public authority with the exercise of this right, except if it is in accordance with the law, for a legitimate social purpose, or for the protection of the rights and freedoms of others

Personal data (particularly medical data) is therefore protected by Article 8 of the ECHR as part of an individual's right to respect for a private life. The Human Rights Act is intended to prevent any communication or disclosure of personal data as may be inconsistent with the provisions of Article 8

ECHR. These rights are also embedded within the Data Protection Act

Page 71 of 74

The Human Rights Act puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

Further information on the Human Rights Act is available from the Ministry of Justice.

https://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf

Obscene Publications Act (OPA) 1959

http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents

OPA has impact on English law as its precedents serve to provide a definition of obscenity that are used in other legal contexts. In addition to the OPA there are a number of other acts that define material that is illegal to hold

- Section 63 of the Criminal Justice and Immigration Act 2008 ("extreme pornography")
- Protection of Children Act 1978
- Video Recordings Act 1984 and 2010
- Indecent Displays (Control) Act 1981
- Customs Consolidation Act 1876, Amendment Act 1887 (Importation of Indecent and Obscene Material)
- Children and Young Persons (Harmful Publications) Act 1955.

Protection of Children Act 1978

http://www.legislation.gov.uk/ukpga/1978/37

An Act to prevent the exploitation of children by making indecent photographs of them; and to penalise the distribution, showing and advertisement of such indecent photographs.

Police and Justice Act 2006

http://www.legislation.gov.uk/ukpga/2006/48/contents

Section 39 and Schedule 11 of the Police and Justice Act amend the Protection of Children Act 1978 to provide a mechanism to allow police to forfeit indecent photographs of children held by the police following a lawful seizure.

Criminal Justice Act 1988

http://www.legislation.gov.uk/ukpga/1988/33/contents

The act contains clauses to create a summary offence of possession of an indecent photograph of a child.

Page 72 of 74

Terrorism Act 2006

http://www.legislation.gov.uk/ukpga/2000/11/contents

The Terrorism Act creates a series of offences in relation to terrorism intended to assist the police in tackling terrorism. Section 19 of the Act imposes a duty on organisations to disclose information to the security forces where there is a belief or suspicion of a terrorist offence being committed. Failure to disclose relevant information can be an offence.

Further information and guidance can be found on the Home Office's official website by clicking the link below.

https://www.gov.uk/government/publications/the-terrorism-act-2006

Digital Economy Act 2010

http://www.legislation.gov.uk/ukpga/2010/24/contents

The act addresses media policy issues related to digital media. The items contained within the act of particular relevance are sections on online copyright infringement and the obligations that internet service providers (ISPs) have to tackle online copyright infringement. It includes an amendment to the Copyright, Designs and Patents Act 1988 to increase the penalty in connection with criminal liability for copyright and performing rights to a maximum of £50,000.

EU Directives

Privacy and Electronic Communications (EC Directive) Regulations 2003 and amendments (2004, 2011 and 2015)

http://www.legislation.gov.uk/uksi/2011/1208/contents/made

An amendment to the Privacy and Electronic Communications Regulations in 2011 obliged websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies. It also regulates organisations that wish to send electronic marketing messages (by phone, fax, email or text).

Further information is available from the ICO website

https://ico.org.uk/for-organisations/guide-to-pecr

EU Data Protection Directive 95/46/EC (Data Protection)

Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within

Page 73 of 74

the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data.

Transfers of personal data from a Member State to a third country with an adequate level of protection are authorised. However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, e.g. the data subject himself agrees to the transfer, in the event of the conclusion of a contract, it is necessary for public interest grounds, but also if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.

European Union Directive 2009/136/EC (Cookie Directive)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

The directive provides obligations on service providers on the security and privacy of users' data. The directive was introduced into English law in the Privacy and Electronic Communications amendments of 2011 in particular with relation to cookies.

European Union Law – The General Data Protection Regulation (GDPR) (EU) 2016/679

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR was adopted on the 27th April 2016 and became enforceable from 25th May 2018 and replaced the 1995 Data Protection Directive 95/46/EC.

Document Control Information

Owner	LLANTRISANT COMMUNITY COUNCIL
Version number	Version 1.0
Original approval date	10TH DECEMBER 2024
Approved By	LLANTRISANT COMMUNITY COUNCIL
Date of last review	10TH DECEMBER 2024
Date of next review	2028

Page 74 of 74