INFORMATION AND DATA PROTECTION POLICY

Approved by Council: **October 2024**

Date to be Reviewed: **April 2025**

Scope

This Policy consists of a suite of inter-linked policies: -

- Information and Data Protection Policy
- Appendix 1 – Information Security Policy
- Appendix 2 – Data Breach Notification Policy
- Appendix 3 – Website Privacy Policy
- Appendix 4 – Subject Access Policy

Introduction

To conduct its business, services and duties, Offa Community Council processes a wide range of data, relating to its own operations and some which it handles on behalf of partners as specified in the Data Protection Act (DPA). In broad terms, this data can be classified as: -

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up (unlikely to be personal or sensitive data under DPA, but confidential nevertheless).
- Confidential information about other organisations because of commercial sensitivity (All Confidential which is also Personal information comes under DPA).
- Personal data concerning its current, past and potential employees, Councillors, and volunteers. (DPA applies).
- Personal data concerning individuals who contact it for information, access its services or facilities or to make a complaint (DPA applies see definition of personal data in 7 below).
- Data passed to a third party (data processor) who undertakes a service or task for the Council, or we have a legal obligation to inform, or we need to share information with (e.g. Pension provider, HMRC) (DPA applies).
- Data processed on behalf of another organisation such as a Trust of which the Council is a trustee, or community partner (DPA applies if that is personal data).

Offa Community Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to any other organisation which it works with and to members of the public. In some cases, it will have

contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

This Policy is linked to our ICT Policy and Data Retention Policy which will ensure information considerations are central to the ethos of the organisation.
The Community Council will periodically review and revise this policy in the light of experience, advice from its Data Protection Officer (DPO), comments from data subjects and guidance from the Information Commissioners Office.

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

Protecting confidential or sensitive information

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

The Data Protection Act seeks to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Community Council with legitimate reasons for using personal information. The policy is based on the premise that Personal Data must be: -

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection.
- Against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Terminology

Data subject means the person whose personal data is being processed. That may be an employee, prospective employee, member or prospective Member of the Council, or someone volunteering to work with it. It may also be someone transacting with it in some way, or an employee, Member or volunteer with one of our clients or partner organisations, or persons transacting or contracting with one of our clients or partners when we process data for them.

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

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

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

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

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

- Organising, adapting or altering it.
- Retrieving, consulting or using the information or data.
- Disclosing the information or data by transmission, dissemination or otherwise making it available aligning, combining, blocking, erasing or destroying the information or data regardless of the technology used.

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Data Protection Officer (DPO) is an enterprise security leadership role required by DPA. DPOs are responsible for overseeing a Council's data protection strategy and its implementation to ensure compliance with DPA requirements.

Offa Community Council processes personal data in order to: -

- Fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- Pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- Monitor its activities including the equality and diversity of its activities.
- Fulfil its duties in operating the business premises including security.
- Assist regulatory and law enforcement agencies.
- Process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- Process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- Undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council. • undertake research, audit and quality improvement work to fulfil its objects and purposes. • carry out Council administration.

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

The Council will ensure that at least one of the following conditions is met for personal

information to be considered fairly processed: -

- Processing is necessary for the performance of a contract or agreement with the individual.
- Processing is required under a legal obligation.
- Processing is necessary to protect the vital interests of the individual.
- Processing is necessary to carry out public functions.
- The individual has consented to the processing • Processing is necessary to pursue the legitimate interests of the data controller.

Particular attention is paid to the processing of any sensitive personal information and the Community Council will ensure that at least one of the following conditions is met: -

- Explicit consent of the individual.
- Required by law to process the data for employment purposes.
- A requirement in order to protect the vital interests of the individual or another person.

Who is responsible for protecting a person's personal data?

The Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Clerk.

- clerk@offacommunitycouncil.gov.uk
- 01978 219562
- Offa Community Council, Luke O'Connor House Resource Centre, 21 Barter Court, Hightown, Wrexham LL13 8QT.

Offa Community Council, as data controller and indeed data processor, remains responsible for compliance with the data protection legislation including the DPA. All Councillors and Officer are expected to apply data protection legislation in their work.

The Council will exercise proper control and management of personal data as this will be fundamental to ensuring, and demonstrating, compliance with the DPA.

Diversity Monitoring

Offa Community Council may monitor the diversity of its employees, and Councillors, to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It may undertake similar data handling in respect of prospective employees. This data will always be treated as confidential. It will only be accessed by authorised individuals within the Council and will not be disclosed to any other bodies or individuals. Diversity information will never be used as selection criteria and will not be made available to others involved in the recruitment process. Anonymised data derived from diversity monitoring will be used for monitoring purposes and may be published and passed to other bodies.

Officer Privacy Notices

The Council will always give guidance on personnel data to employees, Councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Data security and overseas transfers

The Council will ensure the security of personal data. We will make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies.

We will only keep your data for the purpose it was collected for and only for as long as is necessary after which it will be deleted.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us

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

We will not process any data relating to a child (under 13) without the express parental / guardian consent of the child concerned.

Rights of a Data Subject

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

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

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

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

3. The right to have your personal data erased: -

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data

we hold.

- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

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

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

5. The right to data portability: -

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

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

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details). You may access these rights by contacting the Clerk.

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

- You can contact the Information Commissioners Office on 0303 123 1113 or via email or at the Information Commissioner's Office - Wales, 2nd Floor, Churchill House, Churchill Way, Cardiff CF10 2HH.

The Council will always give guidance on personnel data to employees through the Employee handbook.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making information available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the Website and sent to the local media. The Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council

and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its Website or at its Offices.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of Officer, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of Council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure information

The Council will as necessary, undertake checks on both Officer and Members with the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure.

Data transparency

The Council recognises their responsibility to act in accordance with the Local Government Transparency Code (February 2015). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

"Public data" means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery. The Code will therefore underpin the Council's decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops. The principles of the Code are: -

- Demand led: new technologies and publication of data should support transparency and accountability.
- Open: the provision of public data will be integral to the Council's engagement with residents so that it drives accountability to them.
- Timely: data will be published as soon as possible following production. The Council will display at least the amount of data prescribed in the Code on its website and will often

voluntarily exceed this requirement.

The Council will display at least the amount of data prescribed in the Code on its website and will often voluntarily exceed this requirement.

Appendix 1
INFORMATION SECURITY POLICY

Principles and purpose

This Policy sets out the Council's commitment to information security within the Council and provides clear direction on responsibilities and procedures.

Offa Community Council is a Data Controller, as defined under the Data Protection Act 2018, and has registered as such with the Information Commissioner's Office.

Protocols

System security processes and procedures

The Council will provide and maintain security processes and procedures for all key information systems.

The procedures will uphold the principles of confidentiality, integrity, availability and suitability and be assessed for their impact upon other systems and services.

The security procedures will provide preventative measures to reduce the risks to the system, the information held within the system and the service it supports.

A Continuity plan will be developed and maintained for each system to ensure the principles are sustained and enable the continuation of services following failure or damage to systems or facilities.

The Clerk will be responsible for the implementation and promotion of the procedures.

Physical security

Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms should be secured at all times with locked doors as a minimum security requirement.

All documents disclosing identifiable information will be transported in sealed containers e.g. envelopes.

Within their level of authority, Officer will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as laptop, computers, notebooks or mobile phones containing personal or confidential information, should not be left unattended or unsecured and paper records should not be left in public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment.

Logical security

All computerised information and systems will be regularly backed up to a secure environment.

All computerised information systems will be password controlled and all passwords will be

treated with the strictest confidence and users will not divulge their password to any unauthorised person. All sensitive data will be password protected.

Copyright and licenses

The Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the licence agreement.

Disposal and movement of equipment and media

Any media or IT equipment disposed of by the Council will not contain any data or codes that could allow an individual to be identified from it or other confidential information to be accessed. The disposal of equipment will be made under a controlled and documented environment satisfying the requirements of the Data Protection Act 2018 and DPA.

The disposal of media such as disks and memory sticks must ensure that data cannot be recovered. Disposal of such media through the "everyday" waste collection is not permitted. The Council will implement processes to ensure appropriate disposal of such media.

An inventory of all Council computer equipment will be maintained. Details of any equipment or media disposed of or relocated (other than portable equipment) must be recorded.

Computer users

Computer users have responsibility for the security of the equipment in their care and shall not commit any act to compromise the data or Information Security Policy.

Computer users will be made aware of their responsibilities through this policy.

Officer and Councillor responsibilities

The Council will make every reasonable effort to ensure that Officer and Councillors are aware of their responsibilities for the security of information. However, each Councillor or member of Officer is responsible for ensuring that this Security Policy is adhered to and report any breaches of security.

Incident Reporting

Incidents affecting security must be reported to the Clerk as quickly as possible.

Appendix 2
DATA BREACH NOTIFICATION POLICY

Aim

Offa Community Council are aware of the obligations placed on it by the General Data Protection Regulation (DPA) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. The following are examples of data breaches: -

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a data controller or data processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

Breach detection measures

The Council have implemented a range of measures to assist it in detecting a personal data breach and will continue to review and refine these.

The Council will ask its IT Support company to make sure all computers and phones are up to date, make sure our router is an up-to-date quality model, and the firewall and anti-virus software on each computer is current.

The Council will make regular and documented inspections of physical security of premises, rooms and cabinets and ensure documents with confidential or personal information on not left about.

The Council will require our website host to document what they are doing to detect data breaches (typically hacks) and how they report them to you. The Clerk is responsible for this.

Officers are encouraged to regularly check for errors which may result in a data breach and report them to the Clerk or DPO.

The Council will regularly check security monitoring systems should flag up personal data breaches. Officer will be trained to look for to look for: -

- Unusual behaviour from anyone using a system.
- Unauthorised insiders trying to access servers and files.
- Anomalies in outbound network traffic.
- Traffic sent to or from unknown locations.
- Excessive consumption.
- Changes in configuration.
- Hidden files.

- Unexpected changes.

Investigation into suspected breach

If we become aware of a breach, or a potential breach, an investigation will be carried out. All Officers are instructed to contact the DPO immediately a data breach is identified or suspected. This investigation will be carried out by the Data Protection Officer or other person agreed by the Town Clerk and DPO, who will decide on the severity of risk: -

- **Low Risk:** Risk needs to be entered in Breach Register only.
- **Medium Risk:** Breach is required to be notified to the Information Commissioner.
- **High Risk:** Breach will need to be notified to the individual(s) and the ICO

Recording of breaches

The Clerk or other nominated officer records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under DPA. It records the facts relating to the breach, its effects and the remedial action taken.

When a breach will be notified to the Information Commissioner

In accordance with the DPA, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified: -

- A description of the nature of the personal data breach including, where possible: -
    - The categories and approximate number of individuals concerned.
    - The categories and approximate number of personal data records concerned.
    - Contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When a breach will be notified to the individual

In accordance with the DPA, we will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and maybe dependent on the circumstances, be made before the supervisory authority is notified. The following information will be provided when a breach is notified to the affected individuals: -

- A description of the nature of the breach.
- The name and contact details of the Data Protection Officer.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Appendix 3
WEBSITE PRIVACY POLICY

Introduction

This privacy policy governs the privacy of this website and its users who choose to use it.

The policy sets out the different areas where user privacy is concerned and outlines the obligations and requirements of the users, the website and website owners. Furthermore, the way this website processes, stores and protects user data and information will also be detailed within this policy.

The Website

This website and its owners take a proactive approach to user privacy and ensure the necessary steps are taken to protect the privacy of its users throughout their visiting experience. This website complies to all UK national laws and requirements for user privacy.

Use of Cookies

This website uses cookies to better the users experience while visiting the website.

Cookies are small files saved to the users computer's hard drive that track, save and store information about the users' interactions and usage of the website. This allows the website, through its server to provide the users with a tailored experience within this website.

Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors.

This website uses tracking software to monitor its visitors to better understand how they use it. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website but will not store, save or collect personal information.

Other cookies may be stored to your computer's hard drive by external vendors when this website uses referral programs, sponsored links or adverts. Such cookies are used for conversion and referral tracking and typically expire after 30 days, though some may take longer. No personal information is stored, saved or collected.

Visitors to Our Website

When someone visits our website we use a third party service, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow any third party to make, any attempt to find out the identities of those visiting our website.

If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

Contact and Communication

Users contacting this website and/or its owners do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use, as detailed in the Data Protection Act 2018.

Every effort has been made to ensure a safe and secure form to email submission process but advice users using such form to email processes that they do so at their own risk. This website and its owners may use any information submitted to provide you with further information about the services they offer or to assist you in answering any questions or queries you may have submitted. This includes using your details to subscribe you to any email newsletter program the website operates but only if you're express permission was granted when submitting any form to email process.

Your details are not passed on to any third parties.

Email Newsletter

This website does not currently operate an email newsletter program, used to inform subscribers about services supplied by this website.

In compliance with UK Spam Laws and the Privacy and Electronic Communications Regulations 2003 subscribers are given the opportunity to unsubscribe at any time through an automated system. This process is detailed at the footer of each email campaign.

External Links

Although this website only looks to include quality, safe and relevant external links users should always adopt a policy of caution before clicking any external web links mentioned throughout this website. The owners of this website cannot guarantee or verify the contents of any externally linked website despite their best efforts. Users should therefore note they click on external links at their own risk and this website and its owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

Averts and Sponsored Links

This website does not currently contain sponsored links and adverts.

Social Media Platforms

Communication, engagement and actions taken through external social media platforms that this website and its owners participate on are custom to the terms and conditions as well as the privacy policies held with each social media platform respectively.

Users are advised to use social media platforms wisely and communicate / engage upon them with due care and caution with regards to their own privacy and personal details. This website, nor its owners, will ever ask for personal or sensitive information through social media platforms and encourage users wishing to discuss sensitive details to contact them through primary communication channels such as by telephone or email.

This website may use social sharing buttons which help share web content directly from web pages to the social media platform in question. Users are advised before using such social sharing buttons that they do so at their own discretion and note that the social media platform may track and save your request to share a web page respectively through your social media platform account.

Shortened Links in Social Media

This website and its owners through their social media platform accounts may share web links to relevant web pages. By default, some social media platforms shorten lengthy URL's (web addresses).

Users are advised to take caution and good judgment before clicking any shortened URLs published on social media platforms by this website and its owners. Despite the best efforts to ensure only genuine URLs are published, many social media platforms are prone to spam and hacking and therefore this website and its owners cannot be held liable for any damages or implications caused by visiting any shortened links.

Appendix 4
SUCJECT ACCESS POLICY

Introduction

This policy was adopted by the Community Council in order to comply with the requirements of the General Data Protection Regulations (DPA) and Data Protection Act 2018. Data subjects have the right to access personal data held on them by the Council. Details are set out in the Privacy Notice on the Council's website.

This policy is in place to ensure that internal procedures on handling of Subject Access Requests (SARs) are accurate and complied with and includes: -

- Responsibilities (who, what)
- Timing
- Changes to data
- Handling requests for rectification, erasure or restriction of processing.

The Council will ensure that personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered. The Council has implemented standards on responding to SARs.

Upon Receipt of a SAR

The data subject will be informed who at the Council to contact, the Data Controller. The identity of the data subject will be verified and if needed, any further evidence on the identity of the data subject may be requested.

The access request will be verified; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not additional information will be requested.

Requests will be verified as to them being unfounded or excessive (in particular because of their repetitive character); if so, the Council may refuse to act on the request or charge a reasonable fee.

Receipt of the SAR will be promptly acknowledged, and the data subject will be informed of any costs involved in the processing of the SAR.

Whether the Council processes the data requested will be verified. If the Council does not process any data, the data subject will be informed accordingly. At all times the internal SAR policy will be followed, and progress may be monitored.

Data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned may be permitted.

The data requested will be verified to establish if it involves data on other data subjects. This data will be filtered before the requested data is supplied to the data subject; if data cannot be filtered, other data subjects will be contacted to give consent to the supply of their data as part of the SAR.

Responding to a SAR

The Council will respond to a SAR within one month after receipt of the request: -

- If more time is needed to respond to complex requests, an extension of another two months is permissible, and this will be communicated to the data subject in a timely manner within the first month.
- If the Council cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
- If a SAR is submitted in electronic form, any personal data will be preferably provided by electronic means as well.
- If data on the data subject is processed, the Council will ensure as a minimum the following information in the SAR response: o the purposes of the processing; o the categories of personal data concerned: -
    - the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses.
    - where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period.
    - the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; o the right to lodge a complaint with the Information Commissioners Office ("ICO").
- If the data has not been collected from the data subject: the source of such data.
- The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Provide a copy of the personal data undergoing processing.