Coxheath Parish Council

Information and Data Protection Policy

1. Introduction

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

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

1.2. The 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 partner organisations it works with and 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.

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

1.4. 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 village's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

2. Protecting Confidential or Sensitive Information

2.1. The 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.

2.2. The General Data Protection Regulation (GDPR) which became law on 25th May 2018 and like the Data Protection Act 1998, seeks to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Parish Council with legitimate reasons for using personal information.

2.3. **The policy is based on the premise that Personal Data must be:**

2.3.1. Processed fairly, lawfully and in a transparent manner in relation to the data subject

2.3.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

2.3.4. Accurate and, where necessary, kept up to date.

2.3.5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

2.3.6. Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. **Data Protection Terminology.**

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

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

3.3. **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.

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

3.5. **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.

3.6. **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:

3.6.1. organising, adapting or altering it.

3.6.2. retrieving, consulting or using the information or data.

3.6.3. disclosing the information or data by transmission, dissemination or otherwise making it available.

3.6.4. aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

4. Processing Personal Data

4.1. The Council processes **personal data** in order to:

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

4.1.2. 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.

4.1.3. monitor its activities including the equality and diversity of its activities.

4.1.4. fulfil its duties in operating the business premises including security.

4.1.5. assist regulatory and law enforcement agencies.

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

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

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

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

4.1.10. carry out Council administration.

4.2. Where appropriate, and governed by necessary safeguards, the above processing will be carried out jointly with other appropriate bodies from time to time.

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

4.3.1. The individual has consented to the processing.

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

4.3.3. Processing is required under a legal obligation.

4.3.4. Processing is necessary to protect the vital interests of the individual.

4.3.5. Processing is necessary to carry out public functions.

4.3.6. Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

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

4.4.1. Explicit consent of the individual.

4.4.2. Required by law to process the data for employment purposes.

4.4.3. A requirement in order to protect the vital interests of the individual or another person.

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

5.1. 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:

5.1.1. Email: clerk@coxheathparishcouncil.org.uk

5.1.2. Phone: 07947 135782

5.1.3. Correspondence: The Clerk, Parish Office, Coxheath Village Hall, Stocketts Lane, Coxheath, ME17 4PT.

5.1.4. The Council has also appointed an external Data Protection Officer to ensure compliance with Data Protection legislation who may be contacted at: Email: dpo@gdpr-info.com.

6. Data Protection Training

6.1. The Council ensures that those with day-to-day responsibility for enabling the demonstration of compliance with the General Data Protection Regulation (GDPR) and good practice are able to demonstrate competence in their understanding of the GDPR and good practice, and how this should be implemented within Coxheath Parish Council.

6.2. The Council keeps records of the relevant training undertaken by each person who has this level of responsibility.

6.3. The Council also ensures that these staff members remain informed about issues related to the management of personal information, where appropriate, by contact with external bodies. The Council maintains a list of relevant external bodies, the most important of which is the Information Commissioner's Office (www.ico.gov.uk).

6.4. The Council ensures that all staff understand their responsibility to ensure that personal information is protected and processed in accordance with the Council's procedures, taking into account any related security requirements.

6.5. All employees who handle data are given training to enable them to process personal information in accordance with the Council's procedures. This training is relevant to the role that each employee performs within the Council.

6.6. The Clerk is responsible for organising relevant training for responsible individuals and staff generally, and for maintaining records of the attendance of staff at relevant training at appropriate times across the Council's business cycle.

7. Diversity Monitoring

7.1. The Council monitors the diversity of its employees, and Councillors, in order to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It undertakes 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.

7.2. 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.

7.3. 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.

7.4. 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.

8. **Information provided to us**

8.1. 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. In this instance, by transacting with the Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy. However, wherever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Council is able to keep their personal data accurate and up to date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

9. **The Councils Right to Process Information**

9.1. General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e).

9.2. Processing is with consent of the data subject, or

9.3. Processing is necessary for compliance with a legal obligation.

9.4. Processing is necessary for the legitimate interests of the Council.

10. **Information Security**

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

10.2. 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.

11. **Children**

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

12. **Rights of a Data Subject**

12.1. **Access to Information:** an individual has the right to request access to the information we have on them. They can do this by contacting our Clerk or Data Protection Officer:

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

12.3. **Information Deletion:** If the individual wishes the Council to delete the information about them, they can do so by contacting the Clerk.

12.4. **Right to Object:** If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Clerk or Data Protection Officer.

12.5. The Council does not use automated decision making or profiling of individual personal data.

12.6. **Complaints:** If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Clerk, Data Protection Officer or the Information Commissioners Office **casework@ico.org.uk** Tel: 0303 123 1113.

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

12.8. 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.

13. **Making Information Available.**

13.1. 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.

13.2. 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.

13.3. 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.

13.4. Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, 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.

13.5. 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.

13.6. 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.

13.7. 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.

14. Disclosure Information

14.1. The Council will as necessary undertake checks on both staff and Councillors 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 in its integrated quality management system.

15. Data Transparency

15.1. The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). 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.

15.2. "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.

15.3. 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.

15.4. The principles of the Code are:

15.4.1. **Demand led:** new technologies and publication of data should support transparency and accountability.

15.4.2. **Open:** the provision of public data will be integral to the Council's engagement with residents so that it drives accountability to them.

15.4.3. **Timely**: data will be published as soon as possible following production.

15.5. Government has also issued a further Code of Recommended Practice on Transparency, compliance which is compulsory for Local Councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. The Council exceeds this turnover but will nevertheless ensure the following information is published on its Website for ease of access:

15.5.1. All transactions above £100.

15.5.2. End of year accounts

15.5.3. Annual Governance Statements

15.5.4. Internal Audit Reports

15.5.5. List of Councillor or Member responsibilities

15.5.6. Details of public land and building assets.

15.5.7. Draft minutes of Council and committees within one month.

15.5.8. Agendas and associated papers no later than three clear days before the meeting.

16. Breach Notification

16.1. This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

16.2. The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller, or a data processor for the same data processing activity; it must be one or the other.

17. Responsibility

17.1. All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and Councillors of the Council are required to be aware of, and to follow this procedure in the event of a personal data breach.

18. **Procedure – Breach Notification Data processor to Data Controller**

18.1. The Council shall report any personal data breach to the data controller (the Clerk) without undue delay who will pass details to the Data Protection Officer. (GDPR-Info Ltd)

18.2. GDPR-*info* Ltd notifies their contact within the data controller, which is recorded in the Internal Breach Register.

18.3. Notification is made by email.

18.4. Confirmation of receipt of this information is made by email

19. Procedure – Breach Notification Data Controller to Supervisory Authority

19.1. GDPR-Info Ltd shall notify the supervisory authority [ICO] without undue delay, of a personal data breach.

19.2. GDPR-Info Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

19.3. If a risk to the aforementioned is likely, GDPR-Info Ltd shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

19.4. The data controller (Clerk) shall provide the following information to the supervisory authority on a Breach Notification Form:

19.4.1. A description of the nature of the breach

19.4.2. The categories of personal data affected

19.4.3. Approximate number of data subjects affected

19.4.4. Approximate number of personal data records affected

19.4.5. Name and contact details of GDPR-*info* Ltd

19.4.6. Likely consequences of the breach

19.4.7. Any measures that have been or will be taken to address the breach, including mitigation

19.4.8. The information relating to the data breach, which may be provided in phases.

19.4.9. GDPR-*info* Ltd notifies their contact within the supervisory authority, which is recorded in the Internal Breach Register

19.4.10. Notification is made by email.

19.4.11. Confirmation of receipt of this information is made by email.

20. Procedure – Breach Notification Data Controller to Data Subject

20.1. Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject the Council shall notify the affected data subjects without undue delay, [using this form/in accordance with GDPR-*info* Ltd.'s recommendations].

20.2. The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.4 above about sensitive personal information.

20.3. Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

20.4. It would require a disproportionate amount of effort. In such a scenario, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

20.5. The supervisory authority may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.

21. Subject Access Requests

21.1. All personal data processed by the Council is within the scope of this procedure. This procedure excludes personal data that is asked for as a matter of routine by data subjects.

21.2. Data subjects are entitled to ask:

21.2.1. Whether the Council is processing any personal data about that individual and, if so, to be given:

- a description of the personal data;
- the purposes for which it is being processed; and
- details of who will be allowed to see the personal data.

21.2.2. To be given a copy of the information and to be told about the sources from which the Council derived the information; and

21.2.3. Where appropriate, logic involved in any automated decisions relating to them.

22.Responsibilities

22.1. GDPR-*info* Ltd are responsible for the application and effective working of this procedure, and for reporting to the Clerk on Subject Access Requests (SARs).

22.2. GDPR-*info* Ltd is responsible for handling all SARs.

23.Procedure

23.1. Subject Access Requests must be made using our web page https://gdpr-info.com/data-protection-contact-form/.

23.2. The data subject must provide evidence as to identity.

23.3. The data subject must identify the data that is being requested and where it is being held and this information must be shown on the SAR application form.

Note that the data subject is entitled to ask for all data that the Council holds, without specifying that data.

23.4. The date by which the identification checks, and the specification of the data sought must be recorded; the Council has one month from this date to provide the requested information. There are no circumstances in which an extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

23.5. The SAR application is immediately forwarded to GDPR-info Ltd, who will ensure that the requested data is collected within the time frame.

23.6. Collection will entail either:

23.6.1. Collecting the data specified by the data subject, or

23.6.2. Searching all databases and all relevant filing systems (manual files) in Coxheath Parish Council, including all back up and archived files, whether computerised or manual, and including all e-mail folders and archives. The Clerk maintains a data map that identifies where all data in the Council is stored.

23.7. GDPR-info Ltd maintains a record of requests for data and of its receipt, including dates. Note that data may not be altered or destroyed in order to avoid disclosing it.

23.8. GDPR-info Ltd is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either excising identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

23.9. If the requested data falls under one of the following exemptions, it does not have to be provided:

23.9.1. Crime prevention and detection.

23.9.2. Negotiations with the requester.

23.9.3. Management forecasts.

23.9.4. Confidential references given by the Council (not ones given to the Council).

23.9.5. Information used for research, historical or statistical purposes.

23.9.6. Information covered by legal professional privilege.

23.10. The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

23.11. The electronic formats used for responses to SARs are .CSV files.