RUSHBROOKE WITH ROUGHAM PARISH COUNCIL: POLICIES AND PROCEDURES
06 DATA PROTECTION POLICY

Adopted 2018-04-24

---

1. Introduction

1.1 The purpose of this policy is to set out the Council commitment to and procedures for protecting personal data in relation to and to be compliant with the General Data Protection Regulation (GDPR) and any and all other data protection legislation applying in the UK.

1.2 The Council regards the lawful and proper treatment of personal information as vital to service delivery, successful working and to maintaining the confidence of those with whom it deals.

1.3 The Parish Council holds personal data about a range of people including current and former councillors and employees, volunteers, residents, contractors, suppliers, representatives of organisations and councils, job applicants and other stakeholders and individuals for a variety of purposes related to Council business.

1.4 This policy sets out how the Council seeks to manage and protect personal data and to ensure that councillors and staff understand the rules governing their use of the personal data to which they have access in the course of managing, administering and delivering the work of the Council. In so doing it covers the behaviours expected in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to individuals.

1.5 The Council will take all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance and is updated subsequently to reflect the correct and current situation of any individual at any given time.

1.6 The Council is committed to ensuring continued and effective implementation of this policy and expects all councillors, staff, volunteers and third parties to share in that commitment.

1.7 In particular, this policy requires councillors to ensure that the Clerk, as data protection officer (DPO), be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2. Scope

This policy applies to all processing of personal data in all forms and all councillors, staff and volunteers who are required to comply with its terms.

3. Definitions

Anonymisation: data amended in such a way that no individuals can be identified from that data (whether directly or indirectly) by any means or by any person.
Consent: any freely given, positive, specific, informed and unambiguous confirmation of the wishes of the data subject by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her for a particular purpose. Consent must be easy to withdraw and freely given, and provided on an opt-in basis rather than opt-out.

Data Controller: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Rushbrooke with Rougham Parish Council is a data controller and is responsible for ensuring compliance with the requirements specified in this policy.

Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.

Data Protection: the process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Protection Authority: an independent public authority responsible for monitoring the application of the relevant data protection regulation set forth in national law. In the UK, the Information Commissioner's Office (ICO).

Data Protection Officer (DPO): an officer required to be appointed by public authorities to inform and advise organisations about their obligations to comply with the GDPR and other data protection laws; to monitor compliance with the legislation and to be the first point of contact for both supervisory authorities and for individuals whose data is processed. For the Council the Clerk is the DPO and, thereby, has overall responsibility for the day-to-day implementation of this policy.

Data Subject: the identified or identifiable natural (living) person to whom the data refers and about whom the data is processed.

Encryption: the process of converting information or data into code to prevent unauthorised access.

General Data Protection Regulation (GDPR): European Union (EU) legal framework for the protection of personal data effective in the UK from 25 May 2018 (superseding the Data Protection Act 1998). Local councils must comply with its requirements.

Identifiable Natural 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, an on-line identifier, or one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data: any information (including opinions and intentions) which relates to an identified or identifiable natural (living) person, e.g. name, e-mail address, photograph. Identification can be by the personal data alone or in conjunction with any other personal data.

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.

Privacy Notice: a Notice from a data controller to data subjects describing how personal data will be used and what rights the data subjects have.

Process (Processed/Processing): anything done with/to personal data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation: Data amended in such a way that no individuals can be identified from that data (whether directly or indirectly) without a 'key' which permits the data to be re-identified.

Sensitive Personal Data: described in the GDPR as 'special categories of personal data', refers to personal data pertaining to or revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life or orientation, genetic and/or biometric data.

Third Party: any external organisation with which the Council conducts business.

4. Personal Data Collected

4.1 Categories of personal collected by the Council include:

- Names, titles and photographs;
- Personnel details, e.g. staff start/leaving dates, education and work histories, academic and professional qualifications, pension references;
- Contact/client/customer/resident details, e.g. telephone numbers, addresses, e-mail addresses and electoral roll numbers;
- Where relevant to Council legal obligations or services delivered, or where individuals have provided them to the Council, demographic information, e.g. gender, age, marital status, nationality, family composition, and dependants;
- Financial information and identifiers in the context of contracts, purchasing and service agreements, e.g. bank account numbers, payment/transaction

identifiers, policy numbers, VAT numbers, claim numbers, National Insurance numbers, pay and pay records, tax code, tax and benefits contributions, expenses claimed;
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out Council activities, including but not limited to, Website visit histories, meeting attendees, logs of visitors, and logs of accidents, injuries and insurance claims;
- Next of kin and emergency contact information;
- Recruitment information including copies of right to work documentation, references and other information included in a CV or related documents;
- Other staff data (not covered above) including level, performance management information, information for disciplinary and grievance proceedings and personal biographies; and
- Councillor information, e.g. eligibility criteria, register of interests.

4.2 The data, as appropriate and where relevant, may include sensitive personal data (special categories of personal data).

5. Data Protection Officer

5.1 To demonstrate its commitment to data protection, and to enhance the effectiveness of its compliance efforts, the Council, as required by the GDPR, will appoint a data protection officer (DPO).

5.2 The Clerk is the designated DPO and responsible for assisting the controller to monitor compliance with the legislation, this policy and relevant procedures.

5.3 Duties include:
- Keeping the Council and councillors updated about data protection generally including responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Keeping up-to-date with the legislation, relevant case law and issues affecting parish councils and informing the Council as needed.
- Answering questions and queries on data protection from councillors, residents, other authorities, the media, the ICO and others.
- Responding to individuals, particularly councillors, staff and residents, who wish to know what data is being held on them.
- Checking and approving with any third parties which handle Council data any contracts or agreement in relation to data processing.
- Ensuring all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Approving data protection statements attached to e-mails, Council pages on the Rushbrooke with Rougham Website, correspondence and similar.

- Ensuring the implementation of the appropriate documentation to demonstrate GDPR compliance.
- Monitoring the implementation of and compliance with policies, procedures and the GDPR in general.
- Advising the Council on the data protection implications of any projects or initiatives.
- Recommending to the Council any changes to its Risk Register and governance arrangements in the context of data protection.
- Providing prompt and appropriate responses to subject access requests.
- Carrying-out data protection audits.

6. Data Protection Principles

The Council will abide by the principles in the GDPR to govern its collection, use, retention, transfer, disclosure and destruction of personal data. These principles are as follows:

- **Lawfulness, Fairness and Transparency**

The Council will process personal data fairly and lawfully in accordance with individuals' rights, i.e. personal data will not be processed unless the individual whose details are being processed has consented to this happening. The Council will tell data subjects what processing will occur (transparency), the processing will match the description given to the data subject (fairness), and it will be for one of the purposes specified in the GDPR (lawfulness).

- **Purpose Limitation**

The Council will specify clearly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

- **Data Minimisation**

Personal data acquired will be adequate, relevant and limited, i.e. only the minimum amount of data will be collected and kept for the processing purpose specified.

- **Accuracy**

The Council will have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data to ensure that personal data is accurate and, when retained, kept up-to-date.

- **Integrity and Confidentiality**

The Council will, wherever possible, store personal data in a way that limits or prevents identification of the data subject. Personal data will be processed in a manner that ensures appropriate security of that data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and/or organisational measures.

- **Accountability**

The Council, as the data controller, will be responsible for, and be able to demonstrate compliance with the GDPR.

7. Purpose

The Council will use personal data for some/all of the following purposes. To:

- carry out its personnel, administrative, financial, regulatory, payroll and business development functions;
- deliver Council services, i.e. public services, including to understand client needs to provide the services requested;
- confirm the identity of individuals in order to provide some services;
- contact individuals by post, e-mail, telephone or in person;
- enable the Council to build-up a picture of how it is performing;
- prevent and detect fraud and corruption in the use of public funds and, where necessary, for law enforcement functions;
- enable the Council to meet all legal, statutory and governance obligations;
- carry out complaints handling;
- promote the interests of the Council;
- maintain Council accounts and records;
- seek views, opinions or comments;
- promote and notify individuals about Council facilities, services, activities, events, councillors, staff and role-holders;
- send individuals communications which have been requested;
- process relevant financial transactions including grants and payments for goods and services supplied to the Council; and
- support projects and help promote the development of initiatives being pursued by local organisations.

8. Privacy Notice

8.1 Being transparent and providing accessible information to individuals about how the Council will use their personal data is essential. This will be achieved through a Privacy Notice - a vital means of building trust and confidence with individuals.

8.2 Privacy Notices will, as required, be concise, transparent, intelligible and easily accessible. Further, they will be provided free of charge and written in clear and plain language, particularly where aimed at children.

8.3 A Privacy Notice will be supplied at the time personal data is obtained if obtained directly from the data subject. Otherwise the Privacy Notice will be provided within a reasonable period of having obtained the data, and certainly within one month.

9. Lawful Basis for Processing

9.1 The Council will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, the Council will not process personal data unless at least one of the six lawful bases (below) for processing requirements is met and documented.

9.2 Unless an exemption applies, at least one of these will apply in all cases. It is possible for more than one to apply at the same time. For the majority of the time, the Council is likely to rely on consent (but not for councillors and staff); compliance with a legal obligation (which includes performance of statutory obligations); and/or contractual necessity (with contractors etc.).
(a) Consent: the individual has given clear consent for the Council to process his/her personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract the Council has with the individual, or because he/she has asked the Council to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for the Council to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for the Council to perform a task in the public interest, i.e. in the exercise of official authority. This covers public functions and powers that set out in law.
Note: This basis is most relevant to the Council as public authority.
(f) Legitimate interests: the processing is necessary for the legitimate interests of the data controller or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
Note: This basis cannot apply to the Council as it is a public authority processing data to perform official tasks.

9.3 The processing of all personal data must be necessary to deliver Council services; and not unduly prejudice any individual's privacy.

10. Further Processing

10.1 If Council purposes change, or a new purpose emerges which was not originally anticipated, then a new lawful basis may not be needed provided that the new purpose is compatible with the original purpose. However, this does not apply to processing based on consent. Accordingly, the Council will either seek fresh consent which specifically covers the new purpose, or find a different basis for the new purpose.

10.2 In order to assess whether the new purpose is compatible with the original purpose, the Council will take into account:

- any link between the initial and new purpose;
- the context in which the data was collected - in particular, the relationship with the individual and what he/she would reasonably expect;

- the nature of the personal data, e.g. whether it is special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards, e.g. encryption or pseudonymisation.

10.3 The above list is not exhaustive and each situation will be carefully examined but, in general, if the new purpose is very different from the original purpose, would be unexpected to, or would have an unjustified impact on the individual, then it is unlikely to be compatible with the original purpose for collecting the data and the Council will identify and document a new lawful basis to process the data for that new purpose.

10.4 There are some limited circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. The GDPR specifically states that further processing for the following purposes should be considered to be compatible lawful processing operations:

- archiving purposes in the public interest;
- scientific research purposes; and
- statistical purposes.

11. Sensitive Personal Data ('Special Categories of Personal Data')

11.1 In most cases where the Council processes sensitive personal data it will require explicit consent from the data subject to do this - unless exceptional circumstances apply or the Council is required to do this by law, e.g. to comply with legal obligations to ensure health and safety at work. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

11.2 Sensitive personal data is information as to:

- the racial or ethnic origin of the data subject;
- his/her political opinions;
- his/her religious beliefs or other beliefs of a similar nature;
- whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- his/her physical or mental health or condition;
- his/her sexual life;
- his/her genetic data;
- his/her biometric data; and/or
- his her sexual orientation.

11.3 To process sensitive personal data one of the following should apply. It should be noted that more than one of the criteria (below) can apply at the same time.

i. **Explicit consent** of the data subject has been obtained (which can be withdrawn).
ii. **Employment law** - if necessary for employment law or social security or social protection.
iii. **Vital interests** - e.g. in a life or death situation where the data subject is incapable of giving consent.
iv. **Charities, religious organisations and not-for-profit organisations** - to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors.
NB: The Council cannot rely on this lawful basis for processing personal sensitive data.
v. **Data made public by the data subject** - the data must have been made public 'manifestly'.
vi. **Legal claims -** where necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.
vii. **Reasons of substantial public interest** - where proportionate to the aim pursued and the rights of individuals are protected.
viii. **Medical diagnosis or treatment** - where necessary for medical treatment by health professionals including assessing work capacity or the management of health or social care systems.
ix. **Public health** - where necessary for reasons of public health, e.g. safety of medical products.
x. **Historical, statistical or scientific purposes** - where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

11.4 In the Council context the most relevant lawful bases for processing under special category data are likely to be (i), (ii) and (vii), namely:

- Explicit consent from a person;
- Employment law (for staff);
- Reasons of substantial public interest - in performing the public authority role of the Council.

12. Consent

12.1 Consent requires 'clear affirmative action'. Where the Council relies on consent as the lawful basis for processing any personal data, it will only do so where that has been freely given, is specific, informed, unambiguous and able to be withdrawn. As appropriate, it will record how and when the consent was obtained. Signed copies of consent forms will be collected with the issue of general Privacy Notices.

12.2 For councillors and staff, the Council will not rely on consent because consent must be freely given. As it is necessary to process certain personal data for councillors and staff to allow them to perform their roles, and the balance of power between them and the Council is unequal, consent cannot be said to be ‘freely given’. Thus, councillors and staff will not need to sign consent forms but will need to be issued with Privacy Notices.

13. Children's Data

13.1 The Council recognises that the GDPR boosts the protection of children's personal data. The Regulation restricts the age at which data subjects can lawfully give consent, introduces rules for the language used in consent requests targeted at children and regulates the way online ('information society') services obtain children's consent.

13.2 In the Regulation the default age at which a person is no longer considered a child is 16 but, the UK (as permitted by the GDPR) will operate with the adjusted limit of 13 (subject to Parliamentary approval). Data controllers cannot seek consent from anyone under that age but only from a person holding parental responsibility and they must make 'reasonable efforts' to verify that the person providing that consent is, indeed, a parental figure.

13.3 Where services are offered directly to a child, the Council will ensure, as a data controller, that Privacy Notices are written in a clear, plain way that a child will understand.

14. Data Security and Storage

14.1 The Council will adopt physical, technical, and organisational measures to provide for 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 exposed by virtue of, in particular, human action or the physical, technical or natural environment. Measures will include the following:

- when data is stored on printed paper, it will be kept in a secure place where it cannot be accessed by unauthorised personnel;
- printed personal data will, as necessary, be shredded when it is no longer needed;
- personal data stored on a computer will be protected by strong passwords that are changed regularly;
- personal data will not be stored on portable media, e.g. CDs, memory sticks;
- personal data will be regularly backed-up on external hard drives, with one held by the DPO and one by the Chairman of the Council; and
- personal data will not be saved directly to mobile devices such as laptops, tablets or smartphones.

14.2 Where other organisations process personal data in the context of services being delivered to or provided on behalf of the Council the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts or agreements with those third party organisations.

15. Data Retention

15.1 To ensure fair processing, the Council will not retain personal data for longer than is necessary in relation to the purpose(s) for which it was originally collected, or for which it was further processed. What is necessary will depend on the circumstances of each situation, taking into account the reasons that the personal data was obtained, but will be determined in a manner consistent with legal obligations and Council data retention guidelines.

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

16. Subject Access Requests

16.1 Data subjects are entitled (subject to certain exceptions) to request and be provided with access to information held about them. They have the right to be given this information in a permanent form (hard copy) at the earliest and certainly within one month from receipt.

16.2 Data subjects are entitled to obtain, based upon a request made in writing to the Council and upon successful verification of their identity, the following information about their own personal data:

- The purposes of the collection, processing, use and storage of their personal data.
- The source(s) of the personal data, if it was not obtained from the data subject.
- The categories of personal data stored for the data subject.
- The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the personal data or the rationale for determining the storage period.
- The use of any automated decision-making, including profiling.
- The existence of the right to request rectification or erasure of personal data or the restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with the ICO.

16.3 Situations may arise where providing information requested by a data subject would disclose personal data about another individual. In such cases, information will be redacted or withheld as necessary or appropriate to protect that person's rights.

17. Data Subject Rights

17.1 The Council fully acknowledges the rights of individuals, as specified in the GDPR, and will seek to ensure compliance with those rights at all times. When an individual seeks to exercise any of his/her rights, in order to process the request the Council may need to verify the identity of the individual for his/her security.

17.2 Written requests received from data subjects in relation to the rights below will be directed to and dealt with by the DPO who will log each request as it is received and ensure an appropriate and compliant response at the earliest and certainly within one month from receipt.

- **The right to be informed**

Individuals have the right to be given 'fair processing information', usually through a Privacy Notice, which will include an explanation of the lawful basis for the processing of their data, details of data retention periods and their right to complain to the ICO if they believe that there is a problem in the way that the Council deals with their personal data.

- **The right of access (including subject access requests)**

The Council will respond to subject access requests without undue delay and in any case within one month of receipt of the request. Requests will be refused or a 'reasonable fee' charged' should they be manifestly unfounded, excessive or repetitive.

- **The right to rectification (correction)**

The Council will ensure that, when necessary, individuals can readily exercise the right to have their personal data corrected if it is inaccurate or incomplete.

- **The right to erasure (also known as the right to be forgotten)**

The Council will enable the right of data subjects to request the removal or erasure of their personal data, e.g. if it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent. However, if the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and he/she is withdrawing his/her consent.

- **The right to restrict processing**

Individuals have the right to restrict processing of their personal data in certain circumstances, e.g. if a person believes his/her personal data is inaccurate or he/she objects to the processing. If processing is restricted, the Council can still store the data but cannot otherwise use the data.

- **The right to data portability**

Data subjects will have the right to request that their personal data be provided to them (or a third party) in a machine-readable portable format free of charge. The Council will comply with such requests without undue delay and in any event within one month of receipt of the request.

- **The right to object**

Individuals have the right to object to processing in certain circumstances, e.g. if the Council has relied on one lawful ground to process data without consent and

an individual is not happy with this then he/she has the right to object to the Council processing his/her data.

- **The right not to be subject to automated decision-making including profiling**

The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. .

17.3 Individuals also have the right to lodge a complaint with the ICO (Tel.: 0303 123 1113; e-mail: https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF).

18. Sharing Information, Transfers and Third Parties

18.1 It is likely that the Council will need to share personal data with some or all of the following (but only where necessary):

- Council suppliers and contractors, e.g. where a commercial provider is asked to publish or distribute newsletters on behalf of the Council, to maintain database software or host Council information on a Website.
- Other local authorities or not-for-profit bodies with which the Council is engaged.

18.2 The Council will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient.

18.3 There are restrictions on international transfers of personal data. Personal data will not be transferred anywhere outside the UK without reference to the DPO and the acquisition of appropriate advice.

18.4 Specific consent from the data subject will be obtained prior to transferring his/her data outside the European Economic Area (EEA). Any personal data transferred to countries or territories outside the EEA will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union.

18.5 Council information on the Rushbrooke with Rougham Website is accessible from overseas so on occasion some personal data, e.g. in a newsletter, may be accessed from anywhere in the world.

19. Training and Awareness

19.1 Councillors and staff will, as appropriate, receive training on and be made fully aware of this policy. New councillors and staff will be formally briefed as part of the induction process. Further awareness and training will be provided as

needed and certainly whenever there is either a substantial change in the law or Council policy and procedure.

19.2 Training and procedural guidance will consist, at a minimum, of the following elements:

- the data protection principles;
- each person's duty to use and permit the use of personal data only by authorised persons and for authorised purposes;
- the need for, and proper use of, the forms and procedures adopted to implement this policy;
- the correct use of passwords and other security mechanisms;
- the importance of limiting access to personal data by, e.g. using password-protected e-mail and logging-out when systems/PCs are unattended;
- securely storing manual files, print-outs and electronic storage media; and
- ensuring the proper disposal of personal data by, e.g. using secure shredding facilities.

20. Privacy by Design and Default

Privacy by design is an approach to projects and initiatives that promotes privacy and data protection compliance from the start. The DPO will be responsible for conducting any privacy impact assessments and ensuring that all appropriate projects commence with and include a privacy plan which is then maintained throughout the project lifecycle.

21. Data Audit, Personal Data Register and Risk Register

21.1 To confirm that an adequate level of compliance is being achieved by the Council in relation to this policy, the DPO will carry out an annual data protection compliance audit and report on that audit to the full Council.

21.2 That audit will be used to identify and manage risks, and will be used to inform both the Council Risk Register and Council Register of Personal Data. The latter contains information on what data is held, where it is stored and for how long, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

22. Reporting Personal Data Breaches

22.1 A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The GDPR makes informing the ICO and the individuals affected compulsory in certain circumstances, e.g. where there is a high risk to the individuals involved, e.g. through identity theft.

22.2 Where an individual and/or data subject suspects and reports that a potential personal data breach has occurred the DPO will, as soon as possible, seek a description of the circumstances. This allows the Council, through the DPO, to:

- investigate the (potential) failure;
- if a breach is confirmed, to follow the relevant authorised procedure based on the criticality and quantity of the personal data involved;
- effect, at the earliest, any remedial steps necessary;
- notify the ICO if sufficiently serious; and
- document the failure in a register of compliance failures.

22.3 In the event of a severe breach, an extraordinary meeting of the Council will be convened to co-ordinate and manage the response to the breach.

22.4 Data breaches will be reported (where applicable) to the ICO within 72 hours (GDPR requirement) of the breach and will include the potential scope and cause of the breach, mitigation actions planned and measures to address the problem.

23. Failure to Comply

23.1 The Council is fully committed to compliance with this policy and any failure in that regard will be viewed as extremely serious given that such failure, by a councillor or member of staff, will put both the individual and the Council at risk.

23.2 Failure to comply may lead to disciplinary action against staff, a councillor breaching the Suffolk Local Code of Conduct, a formal complaint by a data subject which may lead to action by the ICO and possible fine, and reputational damage to the Council.

24. Revisions

The DPO is responsible, and accountable to the Council, for the maintenance and accuracy of this policy. Notice of revisions, both significant and otherwise, shall be provided to the Council for approval at the earliest opportunity. Below are other Council documents that relate to and/or are referenced by this policy:

- Data Records and Retention Policy
- Standing Orders
- Freedom of Information Publication Scheme

25. Rushbrooke with Rougham Parish Council

Data Protection Officer: Parish Clerk, Mrs P Lamb
Sayesbury House, Ixworth Road, Norton, Bury St Edmunds IP31 3LJ
Tel: 01359 233288
E-Mail: parishclerk@rougham.suffolk.gov.uk
Web: http://rushbrookewithrougham.suffolk.cloud/