GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

January 2021

Formally adopted:	25 January 2021
To be reviewed:	January 2022

CONTENTS

Spaldington Parish Council will hereinto be known in this policy as *'the Council'*

1. INTRODUCTION

i. The Council holds essential personal data to supports its work with community and intends to be open and transparent in its handling of that information. The data held relates to staff, councillors and community and the Council is committed to their privacy, safety and security. To meet that commitment, the Council follows the guidelines set out under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

ii. The Council collects only that personal data in which it has a legitimate interest (ref GDPR Article 6(1)(f). This includes the personal data necessary to meet our legal and business obligations and to ensure good practice in employment and service delivery.

iii. The purpose of this policy is to ensure that:

- Only sufficient, essential personal data is collected, used and stored
- The collection, use and storage of personal data is conducted safely and securely
- Data owners understand and consent to the nature, purpose and extent of data held
- The rights of data owners are fully understood and upheld
- The Council's obligations in the collection, use and storage of data are fully understood and met by staff, trustees and volunteers

2. SCOPE OF THE POLICY

i. This policy covers the collection, processing, and secure storage of personal data. It sets out the protocols for ensuring that the rights of data owners are upheld. It specifies the steps to be taken by the Council to ensure that all staff, volunteers and Councillors involved in the management and delivery of the service understand their obligations in relation to data handling and the procedures to be followed to ensure that personal data remains pertinent and secure. Finally, it outlines the steps to be taken in the event of any data breach; and includes the guidelines for policy review.

ii. The policy is to be used in conjunction with the Council Data Audit (Appendix 1) and the Council Data Risk Assessment (Appendix 2). The Council Data Audit specifies the range of personal data relating to staff, trustees, volunteers and community in which it deems itself to have a legitimate interest; and the purpose for which it is needed.

iii. The Council considers its legitimate interest to be restricted to the personal data that is essential for:

- The safe, fair and legal employment, management and payment of staff
- The safe, fair and legal deployment and management of volunteers
- The safe, fair and legal administration of Councillors' records and expenses
- The administration of the Parish Council statutory responsibilities

iv. Procedures for the safe and secure collection and storage of data are based on a risk assessment undertaken by the Clerk (see Appendix 2). This policy sets out the procedures to be followed by Council staff and Councillors when collecting, processing and storing data; and in the event of any data breach.

3. DATA PROTECTION OFFICER

i. The Council will appoint a Data Protection Officer (DPO) who will be responsible for the administration of this policy and ensuring any data that the Council hold, manages or uses is kept secure

ii. In regard to breaches, the DPO, in consultation with the Chair, will determine if any reporting to the ICO is required. The DPO will be ultimate decision maker but will ensure that notes are made to ensure that any review is able to managed effectively

iii. The DPO will also ensure that any training provision is managed on behalf of the Council.

4. DATA SUBJECTS' RIGHTS / CONSENTS & ACCESS

i. The completion of a contract of employment, or of a volunteer or Councillor registration form implies consent to the collection and use of the personal data provided. However, to ensure their full understanding, data subjects will also be informed about why their personal data is necessary to the Council and how it is kept secure. Data subjects will also be asked explicitly for their written consent to the use of their personal data for its specific purposes.

ii. The rights of data subjects are laid out in the GDPR. The following table sets out data subjects' rights and their reasonable expectations in relation to the Council.

DATA SUBJECTS' RIGHTS		EXPECTATIONS
1.	**The right to be informed**	You have the right to know what information is collected about you, why we need it and what we do with it. The information we collect is restricted to what is provided by you in your application/registration form. Information about why your personal data is collected and how it is used is included in your consent form. This policy document expands on the information given.
2.	**The right of access**	This gives you the right to see the personal information that Council collects about you. Your request should be submitted in writing to the Centre Manager and we may take up to 1 month to respond. From time to time, occasions may arise where it is not possible to allow you access. In this case we must give you an explanation for our decision.
3.	**The right to rectification**	This means that you have the right to ask the Council to rectify any incorrect or incomplete data that we hold about you. Your request should be given in writing to the Centre Manager and it may take us up to 1 month to make the rectifications. In the event that it is not possible for us to rectify the information, we must give you the reasons for this.
4.	**The right to erasure**	You may wish to ask the Council to erase all the personal data we hold about you. Your request should be made in writing to the Centre Manager and we may take up to 1 month. There may be occasions where it is not possible to comply with your request and, in this event, we must give you the reasons.
5.	**The right to restrict processing**	This means that, under certain circumstances, you are able to limit the ways in which the Council handles or uses your personal data. Your written request should be made in writing to the Centre Manager and it may take up to 1 month to comply with your request. If it is not possible to comply with your request, we must give you the reasons for this.
6.	**The right to data portability**	You may wish to transfer the personal data you have given the Council safely and securely to another service.
7.	**The right to object**	You have the right to object to the data held by the Council being used in certain ways. You have the absolute right to object to direct marketing.
8.	**The right not to be subject to automated decision-making or profiling**	The Council does not use automated decision-making or profiling processes.

iii. To exercise their rights, individuals should make a written request to the Clerk. The Council may take up to one month to respond to or comply with any written request. There may be circumstances under which it is not possible to comply with a particular request. In such an event, the Council must give the reasons for this.

iv. Details of who has routine access to data and for what purposes, is set out in the Council Data Audit (see Appendix 1)

5. STAFF TRAINING AND COMPLIANCE

i. Staff and Councillors must understand their obligations regarding the use of personal data. To ensure that all understand their obligations and the procedures to be used in data handling:

a) All staff, volunteers and Councillors should read the Data Protection Policy and Procedures and provide written confirmation that they understand the contents and their obligations in data handling
b) All staff, volunteers and Councillors are given the opportunity to discuss the policy or raise any questions for clarification at team briefing, following its adoption
c) The Clerk and at least two members of the Council should undertake GDPR training and updates as necessary
d) New staff or Councillors are briefed as part of induction
e) Formal training should be given to staff and Councillors at the discretion of the Clerk and Council
f) Sessional staff are asked to sign a confidentiality agreement as part of their contract.

6. DATA SHARING

i. The legitimate interests of the Council inevitably require the transfer of some personal data to other agencies for specific purposes (eg the payment of staff). The Council does not routinely share the personal or work-related data of its staff, volunteers and Councillors or community with any other agencies except for the legitimate purposes outlined in 5.1, 5.2, 5.3 and 5.4 below. Personal data is never shared without the knowledge of the data subject.

ii. **Routine Sharing of Personal Data**

a) Personal staff data required for the administration of salaries, pensions and taxation is routinely shared with any financial or legal advisors and the HMRC when required
b) Personal data of funded community schemes is shared with funding bodies as required
c) Essential medical information relating to all staff, volunteers and Councillors or community may be shared with medical or emergency services personnel in the event of emergency
d) Details of accidents at the Council may be shared with
   - Medical or emergency services personnel in the event of emergency
   - Medical personnel in the event of longer-term consequences of any accident
   - Trustees, HR Advisor, Medical and legal personnel in the event of occupational health or other tribunal
e) Essential personal and medical information, and work-related information (eg sickness, disciplinary, appraisal, holidays and training records) may be shared with Trustees, HR Advisor, medical and legal personnel in the event of dispute or employment tribunal.
f) Monitoring information is collected purely for statistical analysis to ensure fairness in employment and working practice. Individual monitoring information is not shared.

iii. Sharing images

a) From time to time images of staff and Councillors are used to represent the work of the community or Council in marketing and social media. To ensure individuals' safety and privacy:

- No images may be used without the written permission of those individuals shown.
- Individuals may not be identified by name
- No personal details may be included in any texts accompanying the images

- All logins and emails for social media/marketing are registered to the Council with agreed tiered access
- Images may only be used in promotional material or social media with the written approval of the Chair of the Council
- Individuals' consent to the use of images for the purposes stated is renewed annually.

iv. Sharing information with the Council

a) Councillors are responsible for the safe and effective delivery of the service to community and for the strategic direction of the Council. In regular monitoring, evaluation and direction, it may from time to time be necessary for elements of personal information to be shared with the Councillors, for example in staff recruitment or in the event of dispute.

- Information shared with the Council may be discussed only at meetings of the full Council and remains confidential at all times.
- Discussion documents containing sensitive information must kept securely and destroyed when no longer needed
- Minutes of meetings record decisions made without the use of personal data where possible.
- Minutes of meetings are stored electronically with the Clerk

v. Exceptions

a) Circumstances may arise which override the protocols for data sharing set out above. These may include circumstances where there are concerns for the physical or psychological safety of the data subject. Whilst personal data is never shared without the knowledge of the data subject, it may be shared without their consent if there is a legal requirement to do so for safeguarding purposes.

7. DATA PROCESSING

i. The data collected in relation to staff, volunteers and Councillors enables the Council to meet its ethical obligations and legal commitments to

- efficient, safe and fair employment administration and practice
- safe service delivery.

ii. Processing Staff Data

a) Staff personal information is collected for the purposes of efficient employment administration and safe service delivery. This inevitably involves essential personal information for effective communication, staff payment, pension administration and taxation

- Information is provided to the Council on the staff online application form
- The full range of staff data collected and stored by the Council is set out in Appendix 1 (Data Audit)
- Staff data is processed **only** by the Clerk or Chairman
- The Chairman or Clerk will update personal data as required
- At appointment, personal information essential for staff payment, pensions and taxation is shared with the Council's financial advisors via a secure transmission or to the HMRC
- Electronic records are created and stored with the Clerk
- Any paper-based records containing personal data are stored with the Clerk

- Additional data relates to the day-to-day may also be stored in a locked cabinet of the Council's office
- No personal banking details are collected or held by the Council. Monthly payments are made by cheques, signed by the Chair and given or posted to employees
- Access to staff information is restricted to the Clerk and Chairman where necessary.

iii. Processing Councillors' Data

a) Councillors' personal information is collected when required or through normal elections. Only information necessary for effective communication with Councillors and for safe and effective service delivery is collected
b) Limited Councillors' personal data is shared with financial advisors (if necessary) and with the any other statutory body as required by Law
c) Councillors' personal data is provided manually to the Council and the Clerk. The Clerk will ensure this information is kept securely

iv. Processing Community' Data

a) Only data that is essential for effective communication and for safe service delivery is collected from community and held by the Clerk
b) In the case of community who are funded, data is shared with the funding body as required. Data sharing protocols provided by individual funding bodies are strictly followed.
c) Data owned by Local Authority community is shared via the Local Authority
d) Access to community' data is accessed only by the Clerk or Chair

8. DATA SECURITY

i. It is the responsibility of the DPO to ensure that all data held by the Council is secure, meets the policy guidelines as well as any statutory requirements
ii. Paper-based documents are stored in the filing cabinets in the Council office or with the Clerk.
iii. The Clerk will ensure any documents they hold are held securely
iv. Any documentation held in the Council office must also kept securely. The office is kept secure by a lock with keys only held by the Clerk and Chair
v. Electronic data is stored with the Clerk who must ensure it is secure.
vi. Legitimate transfer of personal data to other agencies is undertaken only when the Council is satisfied that their transfer systems are secure and their data protection policies are GDPR compliant.
vii. Personal information is not transmitted by email unless it is considered secure and encrypted
viii. No personal data released by the Clerk or the Council unless in exceptional circumstances and then only with the written permission of the Chair.

9. DISPOSAL OF DATA

i. Data is retained only whilst it is needed. The Data Audit (see Appendix 1) sets out the length of time specific elements of data should be kept.
ii. The Data Audit is reviewed annually and any personal data that is no longer needed is destroyed at that point.
iii. Electronic files are deleted any electronic storage
iv. Paper-based documents are shredded using a cross shredder.
v. Records of the type of information is kept for data audits

10. PROCEDURES TO BE FOLLOWED IN THE EVENT OF DATA BREACH

i. In the event of any data breach, the DPO must be informed immediately and will then take steps to ensure that any risks to individuals are minimized.
ii. The DPO will inform the Chair initially and then the Council at the next meeting
iii. The DPO will decide whether the Information Commissioner's Office (ICO) should be informed
iv. The DPO will lead an investigation to identify what information has been breached and the implications for individual or groups of data owners. In the situation where the DPO is the source of the data breach, the Chair will decide who is the best person to investigate the data breach
v. The DPO (or who deputises) will investigate the source of the breach and the circumstances under it has occurred
vi. The DPO will inform all data owners of the breach and assess the implications for them.
vii. The DPO will take steps to retrieve any lost data, will review the security of the data held and make any recommendations that result.
viii. The DPO will complete a report to Trustees, which will trigger interim policy review.

11. POLICY REVIEW

i. Policy review is undertaken annually and will normally be undertaken by the DPO.
ii. Review of the policy includes review of the Council Data Audit; of the Risk Assessment and of the policies and systems used by those agencies to which the Council transfers personal data.
iii. The policy will be reviewed annually against its key purposes.
- Is the data held still sufficient and essential for the safe and efficient running of the Council?
- Is the data collected still processed and stored safely and securely?
- Does the Council still comply with data protection regulations?

- Are we still satisfied with the Data Protection policies and the security of the systems used by those agencies with which data is shared?
- Do all staff, volunteers and Councillors still understand the policy and their obligations with regard to the safety and privacy of personal data?
- Are there any further training needs?

iv. The Policy Review includes an annual review of the range and nature of data collected and the purpose for which it is required (data audit).
- Is the data audit still accurate and complete?
- Is Council documentation still appropriate for the collection of data?
- What personal data needs to be destroyed?
- Have all staff, volunteers, Councillors and community given their consent to the use of their personal data as outlined?

v. Any data breach will trigger early policy review and a review of the Risk Assessment.

- Under what circumstances did the data breach occur?
- Whose data has been compromised?
- Does the Information Commissioner's Office (ICO) need to be informed?
- How and when were the data subjects informed?
- What are the implications of the data breach for the data subject(s)?
- What steps have been taken to address such implications?

- What was the cause of the data breach and was there any malicious intent?
- Were the electronic or filing systems compromised and have they since been made secure?
- What steps have been taken to reinstate confidence in data security?
- What are the implications for the risk rating?
- What actions need to be taken to minimize the risks of further data breach?
- What resources will be required to support the actions needed?

vi. The policy review may be supported by Centre Self-Assessment using the ICO self-assessment tools.

vii. The policy will be reviewed annually or may be triggered following any data breach or following changes to GDP Regulations – whichever is sooner.

12. **SPECIFIC POLICY REQUIREMENTS**

i. The Council must be registered with the ICO.
ii. A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
iii. The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection. The Council will decide if any additional funding is required
iv. An information audit will be conducted and reviewed at least annually or when projects and services change.
v. Privacy notices must be issued.
vi. Data Protection will be included on the Council's Risk Management Policy.

13. GENERAL INFORMATION

i. One of the greatest challenges currently facing organisations is compliance with the EU's General Data Protection Regulation (GDPR). Because the Council collects and processes personal data belonging to EU citizens, we need to be compliant with the GDPR.

ii. What is GDPR?

a) GDPR stands for General Data Protection Regulation The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.
b) The regulation was made by the European Parliament and the Council of the European Union on 14 April 2016 and implemented from 25 May 2018. It replaces the Data Protection Directive
c) The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
d) The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

iii. What is the Information Commissioner's Office?

a) The Information Commissioner's Office (ICO) is an executive non-departmental public body, sponsored by the Department for Digital, Culture, Media & Sport.
b) The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO is and independent body responsible for enforcing the data protection legislation in the UK.

c) The ICO provides information, checklists and publications to support organisations in handling information well. It also provides training activities. More information about the ICO can be found on its website: Information Commissioner's Office - GOV.UK https://www.gov.uk › Organisations › Information Commissioner's Office

iv. Who's who in data protection?

a) The GDPR identifies data controllers, data processors and data subjects. It also refers specifically to personal data.
b) The data subject is the person whose personal data is being held and used.
c) The term 'Personal data' refers to any information that would help to identify an Individual either directly (such as a name/ID number) or indirectly, particularly when it is used in conjunction with other information such as a date of birth/address/distinguishing feature.
d) The data controller is the organization or person who determines what personal data is needed and the purposes and means of processing that data. The data controller is responsible for ensuring that processors comply with the GDPR.
e) A data processor is the person responsible for processing personal data on behalf of a controller. The GDPR places specific legal obligations on data processors for example, the requirement to maintain records of personal data and processing activities. The data processor has legal liability if responsible for a breach.
f) In this instance, the Council is the data controller and carries ultimate responsibility. The Centre Manager is the data processor. Staff, volunteers, community and trustees are all data subjects.

v. What does it mean that the Council has a 'legitimate interest' in personal data?

a) Legitimate interest (ref GDPR Article 6(1)(f) gives the Council a lawful basis for processing personal date where "processing is necessary for the purposes of the legitimate interests pursued by the organization or a third party." There is an exception to this where the interests of the organization may be "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of persona data, in particular where the data subject is a child" (ICO 2018)