Coney Weston Parish Council

DATA PROTECTION & INFORMATION MANAGEMENT POLICY

DATA PROTECTION

1 ABOUT THIS POLICY

1.1 This policy outlines the standards Coney Weston Parish Council ('the Council') intends to observe in relation to its compliance with the General Data Protection Regulation (GDPR) and Data Protection law.

1.2 The policy is applicable to all councillors and any employees, partners, voluntary groups, third parties and agents authorised by them.

1.3 The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

1.4 This policy applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, mail, microfiche and film.

2 RESPONSIBILITIES

2.1 To operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, customers, contractors, suppliers and partner organisations.

2.2 The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will, therefore, ensure that it treats personal information correctly in accordance with the law. The 6 lawful bases for processing data are Consent, Contract, Legal Obligation, Vital Interests, Public Task & Legitimate Interests

2.3 The Council as a whole is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the Parish Council Clerk, who will undertake information audits and manage the information collected by the Council including the issuing of privacy notices, dealing with requests and complaints raised and the safe disposal of information.

2.4 Councillors who process personal data on an individual basis and are not acting on behalf of the council are likely to be considered data controllers and therefore required to notify the Information Commissioner's Office.

2.5 All councillors and officers who hold or collect personal data are responsible for compliance with data protection legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy.

3 BREACH OF THIS POLICY

3.1 Breach of this policy may result in diciplinary action in accordance with the Council's Conduct or Capability procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal. It should also be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved or legislation is contravened.

Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the District Council's Monitoring Officer.

4 PRIVACY BY DESIGN

4.1 The GDPR requires data controllers to put measures in place to minimise personal data processing and that they only process data that is necessary for the purposes of processing and stored for as long as is necessary.

4.2 The Council will have the appropriate measures in place to determine the basis for lawful processing and will undertake risk assessments to ensure compliance with the law. These measures include the use of Data Protection Impact Assessments (DPIAs), see Appendix 1.

5 CONTRACTS

5.1 Data protection law places requirements on both the Council and its suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means that whenever the Council uses a supplier to process individuals' data on its behalf it must have a written contract in place.

5.2 The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

5.3 The Council is liable for its compliance with data protection law and must only appoint suppliers who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

5.4 If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, or if they will do so as part of the services they provide to the Council, the Clerk must ensure that personal data is managed in accordance with data protection law and this Policy.

5.5 Security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council and reviewed during the contract's life cycle.

5.6 The Clerk will use the appropriate processes, templates and Data Protection Impact Audits when managing or issuing contracts.

6 INFORMATION SHARING

6.1 The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

6.2 Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

6.3 Any Councillor or the Clerk dealing with telephone enquiries must be careful about disclosing personal information held by the Council. In order to manage this the enquirier will be asked to put their request in writing in the first instance.

7 INDIVIDUALS' RIGHTS

7.1 An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR). Information on how an individual can make a SAR can be found in Appendix 2.

7.2 Individuals also have other rights under the Data Protection Act 2018 which are set out in the Council's privacy notices. The Council must respond to individuals exercising their rights within one month.

8 DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

8.1 Personal data can only be disclosed about a third party in accordance with the Data Protection Act 2018.

8.2 If a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek specialist advice before doing so.

9 BREACH OF INFORMATION SECURITY

9.1 The Council understands the importance of recognising and managing information security incidents.This occurs when data or information is transferred to somebody who is not entitled to receive it. It includes losing data or theft of information, unauthorised use of the Council's system to process or store data by any person or attempted unauthorised access to data or information regardless of whether this was successful or not.

9.2 All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate both actual and potential failures and take remedial steps if necessary maintain a register of compliance failures. If the incident involves or impacts personal data it must be reported to the ICO within 72 hours. The Council will follow its Data Breach policy in Appendix 3.

10 IT AND COMMUNICATIONS SYSTEMS

10.1 The Council's IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards users must observe when using these systems and the action the Council will take if users breach these standards.

10.2 Breach of this policy may be dealt with under the Council's Disciplinary Procedure and, in serious cases, may be treated as gross misconduct.

11 EQUIPMENT SECURITY AND PASSWORDS

11.1 The Clerk is responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be set on all IT equipment and passwords must remain confidential and be changed regularly.

11.2 Users must only log onto Council systems using their own username and password. Users must not use another person's username and password or allow anyone else to log on using their username and password.

12 SYSTEMS AND DATA SECURITY

12.1 Users should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

12.2 Users must not download or install software from external sources. Downloading unauthorised software may interfere with the Council's systems and may introduce viruses or other malware.

12.3 Users must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems.

12.4 Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

12.5 Users must inform the Clerk immediately if they suspect a computer may have a virus.

13 E-MAIL

13.1 Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

13.2 It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

13.3 Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

13.4 For the purposes of council business, users must use a designated email account (or only use the email account provided) in order to receive or send email correspondence.

14 USING THE INTERNET

14.1 Users should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content

that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

15 PROHIBITED USE OF COUNCIL SYSTEMS

15.1 Misuse or excessive personal use of our e-mail system or inappropriate internet use will be dealt with under the Council's Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

15.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the Code of Conduct);

(e) confidential information about the Council or any of our staff or our community (except as authorised in the proper performance of your duties);

(f) unauthorised software;

(g) any other statement which is likely to create any criminal or civil liability; or

(h) music or video files or other material in breach of copyright.

16 SOCIAL MEDIA

16.1 This Council's Social Media policy is in place to minimise the risks to our Council through use of social media and can be found here https://coneyweston.suffolk.cloud/coney-weston-parish-council/policies/

17 BRING YOUR OWN DEVICE (BYOD)

The Council must take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. Councillors using their own devices raises a number of data protection concerns due to the fact that these are owned by the user rather than the data controller. The risks the controller needs to assess are:

- The type of data held.

- Where the data may be stored.
- How the data is transferred.
- Potential data leakage.
- Blurring of personal and business use.
- The device's security capacities.
- What to do if the person who owns the device leaves the Council and
- How to deal with the loss, theft, failure and support of a device.

Councillors and officers using their own devices shall have the following responsibilities:

- Users will not lend their device to anybody.
- Users will inform the Council should they lose, sell, recycle or change their device. Users will enable a security pin to access their device and an automatic lock every 5 minutes requiring re-entry of the pin.
- Users will ensure security software is set up on their device and kept up to date.

18 RECORDS MANAGEMENT

18.1 It is necessary for the Council to retain a number of data sets as part of managing council business. The Council shall apply the following framework :

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
□ Minute books	Indefinite	Legal requirement
□ Scales of fees and charges	6 years	Management
□ Receipt and payment account(s)	Indefinite	Archive
□ Receipt books of all kinds	6 years	VAT
□ Bank statements, including deposit/savings accounts	Last completed audit year	Audit
□ Bank paying-in books	Last completed audit year	Audit
□ Cheque book stubs	Last completed audit year	Audit

□ Quotations and tenders	6 years	Limitation Act 1980 (as amended)
□ Paid invoices	6 years	VAT
□ VAT records	6 years generally but 20 years for VAT on rents	VAT
□ Clerk Expenses	6 years	Tax, VAT, Limitation Act 1980 (as amended)
□ Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
□ Insurance policies	While valid	Management
□ Certificates for Insurance against liability for employees	40 years from date on which insurance commenced or was renewed	Best practice
□ Investments	Indefinite	Audit, Management
□ Title deeds, leases, agreements, contracts	Indefinite	Audit, Management

Appendix 1 – DPIA Assessment Checklist

A. Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required.

B. This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

1. Do you need to carry out a DPIA?

(a) What is the objective/intended outcome of the project?

(b) Is it a significant piece of work affecting how services/operations are currently provided?

(c) Who is the audience or who will be affected by the project?

(d) Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals

(e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?

(f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?

(g) Is data being processed on a large scale?

(h) Will the project compel individuals to provide personal data about themselves?

(i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?

(j) Will personal data be transferred outside the EEA?

(k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?

(l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?

(m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)

(n) Is monitoring or tracking or profiling of individuals taking place?

(o) Is data being used for automated decision making with legal or similar significant effect?

(p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)

(q) Is sensitive data being collected including:

(i) Race

(ii) Ethnic origin

(iii) Political opinions

(iv) Religious or philosophical beliefs

(v) Trade union membership

(vi) Genetic data

(vii) Biometric data (e.g. facial recognition, finger print data)

(viii) Health data

(ix) Data about sex life or sexual orientation?

(r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?

(s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?

(t) Will the project require contact to be made with individuals in ways they may find intrusive?

2. Other issues to consider when carrying out a DPIA

(a) In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:

(i) The lawful grounds for processing and the capture of consent where appropriate

(ii) The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing

(iii) Who the data will be disclosed to

(iv) Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)

(v) The internal process for risk assessment

(vi) Who needs to be consulted (Data Protection Officer, data subjects, the Information Commissioners Office ("ICO"))

(vii) Data minimisation (including whether data can be anonymised)

(viii) How accuracy of data will be maintained

(ix) How long the data will be retained and what the processes are for deletion of data

(x) Data storage measures

(xi) Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk

(xii) Opportunities for data subject to exercise their rights

(xiii) What staff or, as appropriate, councillor training is being undertaken to help minimise risk

(xiv) The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

3. **The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.**

4. **If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system.**

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐

2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐

3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐

4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐

5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐

6. Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association. ☐

7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐

8. "New technologies are in use". E.g. use of social media, etc. ☐

9. Data transfers outside of the EEA. ☐

10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐

Appendix 2 SUBJECT ACCESS REQUEST (SAR) POLICY

1. UPON RECEIPT OF A SAR, CONEY WESTON PARISH COUNCIL (CWPC) WILL:

(a) Verify whether CWPC is the controller of the data subject's personal data. If it is not a controller, but merely a processor, CWPC will inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, CWPC may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether CWPC processes the data requested. If it does not process any data, inform the data subject accordingly. At all times make sure the internal SAR procedure is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. RESPONDING TO A SAR

(a) Coney Weston Parish Council will respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

(ii) if the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

I If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) 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 ;

(iv) where possible, the envisaged period for which personal data will be stored or, if not possible, the criteria used to determine that period;

(v) 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;

(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(vii) if the data has not been collected from the data subject: the source of such data;

(viii) 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.

(d) Coney Weston Parish Council will provide a copy of the personal data undergoing processing.

Appendix 3 **Data Breach Policy**

GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or 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

Coney Weston Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a personal data breach -

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Coney Weston Parish Council’s duty to report a breach -

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Coney Weston Parish Council via the Data Protection Officer must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Coney Weston Parish Council must:

i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

ii. Communicate the name and contact details of the Data Protection Officer

iii. Describe the likely consequences of the breach

iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

When notifying the individual affected by the breach, Coney Weston Parish Council must provide the individual with (ii)-(iv) above.

Coney Weston Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processors duty to inform Coney Weston Parish Council
If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Coney Weston Parish Council without undue delay. It is then Coney Weston Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

Records of data breaches -
All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Record of Data Breaches
Date of breach
Type of breach
Number of individuals affected
Date reported to ICO/individual
Actions to prevent breach recurring
To report a data breach use the ICO online system:
https://ico.org.uk/for-organisations/report-a-breach/