Kirton & Falkenham Parish Council

DATA PROTECTION & INFORMATION MANAGEMENT POLICY

Second issue – 26th June 2019

DATA PROTECTION

1 ABOUT THIS POLICY

1.1 This policy outlines the standards Kirton & Falkenham Parish Council (‘the Council’) intends to observe in relation to its compliance with the General Data Protection Regulation (GDPR) and subsequently revised UK 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.

2.3 The Council as a whole is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the Responsible Financial Officer (RFO) 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.

2.6 Procedures containing non-sensitive personal data (eg Emergency Plan) should be managed in such as way that all individuals supplying their own data understand that by doing so their data will be used for the purposes for which those Procedures are intended. If this approach is not followed, the conditions of 2.7 apply.

2.7 Procedures (eg Emergency Plan) containing sensitive personal data must be managed in such a way that written consent is obtained and recorded for that data to be used for the specific purpose of those Procedures.

3 BREACH OF THIS POLICY

3.1 Breach of this policy may result in a detailed review by two parties who are independent of the individual(s) concerned (nominally the Chairman, and RFO, or suitable equivalents) and, in serious cases, may be treated as gross misconduct. 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. It should also be noted that breach of the policy could lead to criminal or civil action if illegal material is involved or legislation is contravened.

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).

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 relevant lead Councillor or Council officer 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 Council officers will use the appropriate processes, templates and DPIAs 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 officer 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.

6.4 CCTV recordings for the Pavilion and Childrens Play area must only be viewed and handled by the System Administrator and one named representative from the Recreation Ground Committee. The recordings must not be shared with other parties apart from authorised bodies (namely The Police, Legal representatives etc) in pursuance of action against individuals suspected of illegal acts which might be captured via CCTV.

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 on the PC website http://kirtonandfalkenham.suffolk.cloud

7.2 Individuals also have other rights under the Data Protection Act 2018 which, if requested, should also be directed via the link on the PC website. The Council must respond to individuals exercising their rights within one month.

7.4 The RFO has primary responsibility within the Council for handling and responding to such requests, although specific tasks may be delegated to other Officers or Councillors.

7.3 Detailed procedures and documentation for dealing with such requests is covered in Appendix A.

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 (Information Commissioners Office) within 72 hours.

10 IT AND COMMUNICATIONS SYSTEMS

10.1 The Council does not own IT and communications systems (with the exception of a small number of PC devices used for Council activity eg Clerk's allocated PC). However the approach described in Sections 10 to 15 are intended to promote effective communication and working practices. This policy outlines the standards users should observe when accessing electronic systems (eg Council website, Mailchimp server, Social media platforms etc) and the action the Council will take if users breach these standards.

10.2 Breach of this policy may result in a detailed review by two parties who are independent of the individual(s) concerned (nominally the Chairman, and RFO, or suitable equivalents) and, in serious cases, may be treated as gross misconduct.

11 EQUIPMENT SECURITY AND PASSWORDS

11.1 Councillors and officers are responsible for the security of any 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 should be set on all Council and own use IT equipment used in the pursuance of Council business and passwords must remain confidential, and if any records are kept, they should be in password protected files. The exception to confidentiality of passwords is that in order to maintain data integrity for single password systems (eg in the case of long term absence, illness, death etc), these passwords should be shared with one other nominated person (Officer or Councillor), who are also required to store them securely. Examples of such systems are: Clerk's PC and email password; Mailchimp; Finance tools; Emergency Plan and associated data etc

11.2 Users must only log onto multi-user Council systems (eg Council website) 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.

11.3 CCTV recording equipment and recordings must be kept in a locked cupboard in the Pavilion, with key access controlled by a named representative of the Recreation Ground Committee

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). This mostly applies to the Council's website, Finance tools etc

12.2 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.

13 E-MAIL

This section relates to email use in fulfilling roles as part of the Council (Clerk, RFO, Councillor etc)

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.

14 SOCIAL MEDIA

14.1 This policy is in place to minimise the risks to our Council through use of social media.

14.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Whisper, Instagram, Vine, Tumblr and all other social networking sites, internet postings and blogs. It applies to use of social media for Council purposes as well as personal use that may affect our business in any way.

14.3 Users should avoid making any social media communications that could damage the Council's interests or reputation, even indirectly.

15 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

15.1 Users should make it clear in social media postings if they are speaking on behalf of the Council.

15.2 In all communications users should be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

15.4 Users may be required to remove any social media content that the Council believes constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

16 RECORDS MANAGEMENT

16.1 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	Archive
§ 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

§ Paid cheques	6 years	Limitation Act 1980 (as amended)
§ VAT records	6 years generally but 20 years for VAT on rents	VAT
§ Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)
§ Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
§ Wages books	12 years	Superannuation
§ Insurance policies	While valid	Management
§ Certificates for Insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (SI. 2753), Management.
§ Investments	Indefinite	Audit, Management
§ Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
§ Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)

16.2 Printed and other paper documentation which contains sensitive personal data must be maintained in locked storage eg filing cabinet.

16.3 Personal data will be kept only as long as is necessary to fulfill the specific purpose for which it has been acquired, after which it will be deleted (or otherwise disposed of).

16.4 CCTV images are kept on hard drives within the Pavilion and are overwritten after approximately four weeks. Images will nly be retained longer than this period if required in pursuance of processing potential or actual criminal activity by the relevant authorities.

17 VALIDATING PERSONAL DATA

Where personal data is obtained and recorded, the process for ensuring this data is correct and current should be managed either:

- directly by individuals accessing specific on-line systems to correct that data (eg Mailchimp), or if they are unable to do so, via the published email account for the system administrator (Data Processor) to do so on their behalf. Or,

- as part of an annual review of the data contained in a particular document, procedure or system (eg Emergency Plan). This shall be undertaken by the Data Processor for that document, procedure or system.

End of document

Appendix A – PROCEDURES FOR DATA REQUESTS AND PERSONAL RIGHTS

1. Upon receipt of a SAR

Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.

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

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

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

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

Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

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

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.

Responding to a SAR

Respond to a SAR within one month after receipt of the request:

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

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.

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

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

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[1] or EU model clauses[2];

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

the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

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

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

the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Provide a copy of the personal data undergoing processing.

Subject Access Requests Policy

What must I do?

1. ***MUST***: On receipt of a subject access request you must **forward** it immediately to the RFO (Responsible Finance Officer) for recording and processing.
2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation
3. ***MUST***: A member of staff, and as appropriate, councillor, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access.
4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. ***MUST***: We must **respond** within one calendar month after accepting the request as valid.

[1] "Binding Corporate Rules" is a global data protection policy covering the international transfer pf personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant

[2] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

6. ***MUST***: Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
7. ***MUST***: Councillors and managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. ***MUST***: Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

How must I do it?

1. Notify RFO upon receipt of a request.
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):

   Current UK/EEA Passport

   UK Photocard Driving Licence (Full or Provisional)

   Firearms Licence / Shotgun Certificate

   EEA National Identity Card

   Full UK Paper Driving Licence

   State Benefits Entitlement Document*

   State Pension Entitlement Document*

   HMRC Tax Credit Document*

   Local Authority Benefit Document*

   State/Local Authority Educational Grant Document*

   HMRC Tax Notification Document

   Disabled Driver’s Pass

   Financial Statement issued by bank, building society or credit card company+

   Judiciary Document such as a Notice of Hearing, Summons or Court Order

   Utility bill for supply of gas, electric, water or telephone landline+

   Most recent Mortgage Statement

Most recent council Tax Bill/Demand or Statement

Tenancy Agreement

Building Society Passbook which shows a transaction in the last 3 months and your address

3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.
4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.
5. Make this clear on forms and on the council website
6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.
7. A database will be created and maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.
8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

Sample letters

1. All letters must include the following information:

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[3] or EU model clauses[4];

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

the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

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

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

the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

=================

Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

=================

Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[3] "Binding Corporate Rules" is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[4] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

=================

Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is ‘legally privileged’ because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely”