	Policy Name: DATA PROTECTION POLICY & PROCEDURE Policy Reference: FCC-05		
Author:		Vicky Mote (Clerk)	
Version	Date Adopted	Next Review Date	Reason for change (new, full rewrite, minor change) to reflect legislation.
1	18-05-23	May 24	Rewrite

Table of Contents

POLICY 2
1. Personal data: 2
2. Sensitive data: 2
3. Commercially sensitive data: 2
4. Why this policy exists: 2
5. Data Protection Law: 2
6. Responsibilities: 3
7. Responsibility for Data Management 3
7.2 Data Protection Officer 3
7.2 Staff of the Council 3
7.3 Members/Councillors 3
PROCEDURE 4
1. SCOPE OF DOCUMENT: 4
2. DEFINITIONS 4
2.1 Data Controller: 4
2.2 Data Protection Officer: 4
2.3 Personal Data: 4
2.4 Sensitive data: 5
2.5 Commercially sensitive data: 5
2.6 Processing: 5
2.7 Subject Access Requests: 5
2.8 Data Sharing Agreements: 5
2.9 Data Processing Agreements: 5
2.10 Privacy notice: 5
3. RESPONSIBILITIES: 5
3.1 Data Controller: 5
3.2 The Data Protection officer: 6
3.3 The Clerk: 6
3.4 Staff: 6
3.5 Members (Councillors): 8
4. DATA PROTECTION OFFICE CONTACT DETAILS 9

POLICY

Fairfields Community Council will comply with the Data Protection Act (DPA) 2018 and provide a framework of rights and duties designed to safeguard personal and sensitive data. Failure to comply with the demands of the Act constitutes a criminal offence.

1. Personal data:

Fairfields Community Council needs to gather and use certain types of personal information about individuals. This can include service users or suppliers, business contacts, employees and other people the Council has a relationship with or may need to contact. This policy describes the principles and legal reasons for which personal data will be collected, handled and stored to meet the Council's data protection standards and to comply under the legislation. Personal data means information about a living individual from which they can be identified, and includes data held on the electoral register, details of customer's names, addresses and plot holdings, databases of names, National Insurance Numbers, bank account details, staff records, CCTV footage and any other information held by the Data Controller. It includes sensitive data and expressions of opinion about the individual. It should be noted this list is not an exhaustive one.

2. Sensitive data:

Includes, but is not confined to, information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or convictions. Processing of data includes the acquisition, storage, manipulation, transfer, deletion and disclosure of the data, and applies to both electronic data and data held on manual records.

3. Commercially sensitive data:

Commercially sensitive data is data the council holds about suppliers' quotations, or contracts with the Council. It does not fall under the categories of personal data covered by the Data Protection Act 2018, but nevertheless exposure of this data poses a risk, and it has therefore also been considered as part of the data protection measures of the Council.

4. Why this policy exists:

This Data protection policy ensures that Fairfields Community Council:

4.1 Complies with data protection law and follow good practice.
4.2 Protects the rights of staff, residents, customers, partners and stakeholders.
4.3 Is open about how it stores and processes individuals' data.
4.4 Protects itself from the risks of a data breach.

5. Data Protection Law:

The Data Protection Act 2018 describes how organisations must collect, handle and store personal information. This applies regardless of whether data is stored electronically, on paper or on other materials. To comply with the regulations, personal information must be collected in an open and fair manner and used fairly, stored safely and not disclosed unlawfully. Personal data must:

5.1 Be processed fairly, lawfully and transparently.
5.2 Be obtained only for specified, explicit and legitimate purposes.
5.3 Be adequate, relevant and not excessive.
5.4 Be accurate and kept up to date.
5.5 Not be held for any longer than necessary.
5.6 Be protected ***with Integrity and confidentiality***.
5.7 Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

The Council will take every effort to ensure that the above principles are built into its daily practices and activities.

6. Responsibilities:

Everyone who works or volunteers for Fairfields Community Council, as well as members of the Council, have some responsibility for ensuring data is collected, stored and handled appropriately in line with this policy. Fairfields Community Council will ensure that:

6.1 Everyone processing personal information is appropriately trained to do so.
6.2 Everyone processing personal information is appropriately supervised.
6.3 Enquiries are dealt with courtesy.
6.4 It will regularly review and audit the ways it holds, manages and uses personal information.
6.5 It assesses and evaluates its methods and performance in relation to handling personal information.
6.6 All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.
6.7 All councillors are aware of the principles of data protection and agree that they will take every effort to ensure that once data is transferred to them from the Council, they engage in proper Data Protection practices.

7. Responsibility for Data Management

7.1 The Data Controller

Under the Act, the Data Controller is Fairfields Community Council. This means the Council will be responsible for ensuring that data is collected where deemed necessary, stored efficiently and securely and for how long. As data controller the Council ultimately determines for what purposes personal information is held and what it will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for. The Town Clerk will carry out the active duties of the Council for data control and staff will handle various aspects of data management and data processing.

7.2 Data Protection Officer

Fairfields Community Council will appoint a Data Protection Officer, who will be responsible for data queries, investigations around misuse of data, and who will act with the Data Controller in ensuring the Council is prepared for the requirements of the Data Protection Act 2018.

7.2 Staff of the Council

Staff of the Council will be responsible for data processing and data management and will act under the guidance of the Clerk of the Council.

7.3 Members/Councillors

Data held by Councillors in their personal (home or personal electronic devices) records, unless generated by the Council, is not considered data held by the Council. Such data is to be managed individually by Councillors who will wish to register with the ICO as data controllers.

PROCEDURE

The Data Protection Act 2018 has placed additional obligations on the processing of personal data and created further rights for people whose personal data is processed.

1. SCOPE OF DOCUMENT:

This document is for members of the Council and employees/volunteers working at the Council and for the Data Protection Officer.

It applies to all personal data that the Council holds relating to identifiable individuals. This can include:

a) Names of individuals.
b) Postal addresses.
c) Email addresses.
d) Telephone numbers.
e) IP addresses.
f) Other data as deemed necessary/ bank accounts.

It sets out our data protection procedures to assist you in handling data correctly in carrying out your duties. If we do not comply with the Data Protection Act 2018 (DPA 2018) we may be subject to extremely large fines or even criminal charges.

The Council is committed to protecting the personal data of individuals from unintended loss, damage, modification, destruction, disclosure or other security risks and to processing personal data fairly in accordance with current data protection legislation.

It is essential that all Members, staff and volunteers maintain the integrity of individuals' personal data by complying with the DPA and this procedure. Failure to observe this procedure will represent a breach of employee employment terms or the Councillors' Code of Conduct.

This procedure is not intended to be a fully comprehensive guide to the DPA 2018 and any specific data protection issues should be referred to our Data Protection officer, Vicky Mote, for advice. It should be read in conjunction with the Data Protection Policy, and the Privacy Notice.

2. DEFINITIONS

Data Protection legislation has a language of its own. Some helpful definitions are set out below to assist in your understanding of this Procedure:

2.1 ***Data Controller:*** The Data Controller is Fairfields Community Council. The Council is the body who decides the purposes for which and the way in which personal data is processed, but the Clerk exercises their role as Proper Officer of the Council in ensuring that this takes place.

2.2 ***Data Protection Officer:*** The person appointed by Fairfields Community Council to handle anything and everything to do with Data Protection enquires, breaches of information, and who will review of procedures and practices for the Council, for all its members.

2.3 ***Personal Data:*** means information about a living person who can be identified by that information or by that information together with other information that the Data Controller has

or is likely to obtain. This can include such data as: Names of individuals, postal addresses, email addresses, telephone numbers, IP addresses, CCTV, some photographs, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2.4 ***Sensitive data:*** means data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.5 ***Commercially sensitive data:*** means data that the council holds about suppliers' quotations, or contracts with the Council. It does not fall under the categories of personal data covered by the Data Protection Act 2018, but nevertheless exposure of this data poses a risk, and it has therefore also been considered as part of the data protection measures of the Council.

2.6 ***Processing:*** means any operation carried out by the Council or its staff relating to the collection, storage, disclosure or transfer to third parties and the archiving and ultimate deletion. It covers both electronic data and data held on manual records.

2.7 ***Subject Access Requests:*** A request, submitted formally by any person (Data Subject) asking for details about what information is stored by the Data Controller, how it's stored and handled and whether it's shared with third parties.

2.8 ***Data Sharing Agreements:*** Formal agreement between the Council and bodies that will need to hold and process data given to them by the Council for service provision (Financial services, hosted services, Primary Authority, service users, Councillors, etc) that details the scope of data held, for what purpose, guidelines for processing, storing and transporting the data and responsibilities under the DPA 2018.

2.9 ***Data Processing Agreements:*** agreement between Council as a Data Controller with individuals or bodies who give information to the Council for processing purposes (residents' complaints, groups advertising on the Council website, information from Councillors, etc.)

2.10 ***Privacy notice:*** a document that is available and answers the questions: **What** data is collected **Why** is the data collected and **Where** will data be collected from and stored.

3. RESPONSIBILITIES:

The Council expects all staff/volunteers and Members to use computers, email and the internet responsibly and in accordance with the data protection principles.

Staff and Members are expected to adhere to this procedure and to ensure that they, and those for whom they hold responsibility, adhere to this policy and protect computer systems and personal data from security risks.

3.1 ***Data Controller:***

Under the Act, the Data Controller is Fairfields Community Council. This means the Council will be responsible for:

a) Ensuring that data is collected where deemed necessary and where it is legally allowed to be collected, that it is stored efficiently and securely and for how long.
b) Determining for what purposes personal information is held and what it will be used for.
c) Taking Responsibility for notifying the Data Protection Agency of the data it holds or is likely to hold, and the general purposes that this data will be used for.
d) Ensuring that where data is to be shared, there are the appropriate agreements in place that set out the legal obligations on how data is obtained, handled and stored.
e) Ensuring that the DPA 2018 is upheld in every aspect and that Data Subjects rights are not infringed.

f) Ensuring staff/volunteers and Members are trained sufficiently to ensure integrity of the data obtained/held.
g) Appointing a Data Protection Officer.
h) Advising the Information Commissioner of any breaches of data held.
i) Reviewing all data protection related policies and procedures in line with an agreed schedule.
j) When new services or activities are planned, the Data Controller will carry out Data Protection Impact Assessments on these to ensure that Data Protection is designed into the systems.

3.2 The Data Protection officer:

a) Keeping the Council updated about data protection responsibilities, issues and risks identified under the cover of the DPA 2018.
b) Handling any data protection questions from staff and members where they have any doubts as to whether or not the processing of personal data that they require to carry out in the course of their employment complies with the Act.
c) Giving guidance on appropriate levels of security for data.
d) Dealing with the Subject Access Requests from individuals to see the data held about them.
e) Checking and approving any third-party contracts and agreements that may handle sensitive information.
f) Issuing Data Sharing Agreements or Data Processing Agreements where necessary and ensuring that these are signed.
g) Arranging ongoing data protection training and advice for people covered by the Data Protection Policy.
h) Maintaining the document retention policy and ensuring document retention takes place according to the policy.

3.3 The Clerk:

a) Approving any data protection statements attached to communications such as emails and letters for staff.
b) Addressing data protection queries or requested comments from newspapers, journalists or media outlets, in conjunction with the Chair of the Council.
c) Ensuring the privacy notice is current.
d) Updating the data mapping document annually and reviewing its effect on policy and procedures.
e) Ensuring data is be backed up frequently and regularly.

3.4 Staff:

a) When data is stored on paper, it should be kept in a secure place where unauthorised people cannot have access to the information. Office boundaries must remain secure.
b) When not required the paper or files should not be displayed in the open and that paper data and printouts are not left where unauthorised people can see them (such as on a printer or in an in tray.)
c) When working with personal data, staff who leave their office/desk space for any extended period of time should ensure that their computers are switched off when left unattended.
d) A clean desk policy should be followed.
e) Data printouts should be archived according to the data retention policy and then securely cross shredded at the end of the archive period and disposed of securely.
f) When data is stored electronically it must be protected by strong passwords.
g) Data is only to be saved on designated drives and servers on not to desktops, laptops or portable devices. If necessary to save onto the Council's laptop, make sure that appropriate security measures have been implemented following a risk assessment. This will comprise an encryption and security system.

h) If data has to be stored on removable media (CD, DVD, mini hard disc drives and USB flash memory data sticks) these should be kept securely when not in use and for a limited period.
i) Personal data of a sensitive nature is to be sited in a secure location, away from the general all access server and saved regularly onto a stand-alone hard drive.
j) No personal data may be kept at home, unless place of work, or on employees' own devices.
k) Data held should be regularly reviewed and updated if it is found to be out of date. Staff should take every opportunity to ensure data is current for any contact they deal regularly with and should get into the habit of regularly confirming contractors/service providers, user groups, stakeholder details when making contact.
l) Staff must annually, normally in December, review all their folders on the server to ensure that old unused data is deleted.
m) Staff must remove all received and sent emails that are older than 2 years.
n) Staff must notify changes of name, address, telephone number, bank and marital status to the Data Protection Officer as soon as possible.
o) No duplicate records are to be made of any data relating to individuals for any purpose where a centralised filing option is available.
p) Personal data must not be transmitted over the Internet unless appropriate encryption methods are used.
q) Personal data must not be sent to a third party on portable storage media or in paper form by conventional post. A secure delivery service must be used.
r) Data must be encrypted before being transmitted electronically. Failing this, data may be transmitted by fax for tele pay purposes if this is the only method allowed.
s) Staff who are involved with third parties that process personal data (PfP, bank, Payroll, Tele-debit system, pension providers, public works, accounting bodies, external service providers, etc) must ensure that a Data processing agreement is in place. This may form part of conditions of hire. (Speak to the Data protection Officer to ascertain that a signed agreement is in place).
t) Staff who send confidential personal data or commercially sensitive data to Members must use pink paper and pink font colour for information posted under the website secure members area, so all persons know this is information that is sensitive.
u) Staff who send pink paper data as part of the working papers to councillors must ensure that these emails are subject headed with the word 'Confidential.'
v) When dealing with quotations from suppliers, be aware that if the quotation itself is part of the working papers, this breaches data security, unless issued on pink papers. An alternative is to supply quotes to councillors in a table where the supplier is not mentioned, and simply refer to suppliers as A, B or C along with their price. Another alternative is to redact the name and logo of the supplier on the quotation.
w) Pink papers must be handed out at meetings, and not left with Councillor packs in the foyer.
x) Emails containing personal/sensitive data that are necessary to include in working papers for meetings must have the data removed by pasting the body of the email into a Word document and leaving off the person's name, email address etc. The email can then be anonymised. Please remember that working papers may become public once the meeting has taken place if they are subject to a Freedom of Information request.
y) Any survey responses sent electronically via email (that will contain personal data) must be logged onto the appropriate file on the server which can be collated and deleted once the responses have been analysed.
z) Staff must not procure personal information from the Council and/or use it without its consent as to do so is likely to constitute a criminal offence under the Act.
aa) Provide all assistance to the Data protection Officer in the conduct of any audit or preparing a response to a subject access request.
bb) Where no procedures are set out explicitly, staff should exercise a degree of care over the personal data that you process by considering the harm that may result were the information to be disclosed unintentionally.

cc) Notify the Data Protection Officer immediately should you detect any potential or actual breach of the Act.
dd) Data held should be annually reviewed and updated if it is found to be out of date.
ee) A subject access request cannot be processed by any staff. Such requests must be immediately passed on to the Data Protection officer for processing.
ff) Seek advice from the Data Protection Officer or the Clerk
gg) Staff may not use or insert USBs into office computers for any reasons, other than for the purpose of recording slides for a formal presentation or backing up important personal data held on staff members. Permission must be given by the clerk for this to occur.

3.5 Members (Councillors):

Members should note that individually they are not the same corporate body for data protection purposes as the Council. When acting at meetings, they are the corporate body, but in their own homes, or at other venues, Councillors are individuals representing residents, and they have individual data protection responsibilities which are separate from the Council's data protection responsibilities. It is suggested that Councillors register independently with the Data Protection Agency. Members should note the following when acting as individual councillors:

a) When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot have access to the information.
b) Note that most working papers do not include data that must be protected (personal data.) If such data is issued by the office this will be on pink papers. Members must not share any data they receive in working papers that is on pink paper or in pink font colour as this information is sensitive. Pink papers must be kept in a secure place, or if issued by email, emails must be secure and password protection must apply to the device.
c) When working with personal data on your device (desktop computer, laptop, iPad, phone or any other portable device) it is recommended that Members should ensure that the document containing the data is closed down and that the screen of their device is always locked when left unattended or not in use.
d) When personal data is stored electronically it must be protected by strong passwords and the device it is stored on must have anti-virus software to prevent hacking.
e) Personal data should not be shared informally.
f) If personal data has to be stored on removable media (CD, DVD, mini hard disc drives and USB flash memory data sticks) these should be kept securely when not in use, the data kept for a limited period and the device protected by anti-virus software.
g) Personal Data should be backed up frequently and regularly.
h) Personal Data held should be regularly reviewed and deleted. The Council recommend that emails for example are only held for a maximum of 2 years, even in archived folders.
i) Members who receive emails from residents or local organisations that contain personal data which they wish to pass to the clerk or other staff will need to note that this information is being passed to another body, i.e., the Council, and it will therefore be subject to the Council's Data Protection policy, and procedures.
j) Members may receive emails from the Council which includes personal data. For this reason, Members must sign a Data Sharing Agreement.
k) Members may share information with the Council, such as private telephone numbers, which are not in the public domain. For this reason, Members must sign a Data Processing Agreement that allows the Council to hold this information.
l) Personal data must not be transmitted over the Internet or by phone unless appropriate encryption methods are used.
m) Personal data must not be sent to a third party on portable storage media or in paper form by conventional post. A secure delivery service must be used.

n) Personal information on individuals/groups/companies cannot be procured from the Council and/or used without its consent as to do so is likely to constitute a criminal offence under the Act.
o) Members should advise the Data Protection Officer of any changes to their contact details or to any other details that may be of relevance.
p) Notify the Data Protection Officer immediately should you detect any potential or actual breach of the Act. The Data Protection Officer will help you to log the breach with the Data Protection Agency.
q) Where no procedures are set out explicitly, Members should exercise a degree of care over the personal data that you process by considering the harm that may result were the information to be disclosed unintentionally.
r) Members need to identify whether Data Subject requests are aimed at them individually or at the Council. Where they are for the attention of the Council such requests must be immediately passed on to the Data Protection officer for processing and should not be answered in a personal capacity. The Data Protection officer can also act for Members who receive a Data Subject request on information that is for their personal attention, and can assist in reporting the breach of data, and undertaking investigations.

4. DATA PROTECTION OFFICE CONTACT DETAILS

Name: Vicky Mote
Telephone: 01908 736899
Email: clerk@fairfields-pc.gov.uk