DATA PROTECTION & PRIVACY POLICY

Adopted by Council at the Annual Meeting of Council on
16th May 2023

Introduction

The Data Protection Directive 95/46/EC has been in force in UK law since 2000. The directive and resulting UK law will be replaced by Regulation (EU) 2016/679 in 2018, known as GDPR.

The Privacy and Electronic Communications Regulation, known as PECR, has been in place since 2003 and became enforceable by the ICO in the UK in 2011. The ICO can enforce punitive monetary penalties for breaches of PECR, GDPR regulations or the UK DPA.

Campbell Park Community Council is fully committed to comply with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000. This UK law is superseded by the EU General Data Protection Regulation on May 25, 2018. Furthermore, the EU Privacy in Electronic Communication Regulations have been in force in the UK since 2003. The two pieces of legislation combined give protection to all living EU citizens on how their personal data is processed, shared and used by public organisations, charities, local government and businesses.

The Council will therefore follow policy and procedures that aim to ensure that all employees, elected or co-opted members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the data protection and privacy legislation that is currently in force.

Statement of policy

In order to operate efficiently, The Community Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the legislation to ensure this.

The Community Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully, fairly and correctly.
To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the current legislation.

The principles of data protection

The legislation stipulates that anyone processing personal data must comply with **Eight Principles** of data protection law. These principles are legally enforceable and may in some cases attract monetary penalty or criminal proceedings if ignored or not followed. In the UK, enforcement is the responsibility of the

Information Commissioners Office. This UK government agency also provides all the documentation and advice required to enable organisations such as Community Councils to fully comply.

The principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The legislation provides conditions for the control and processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Campbell Park Community Council is both a Data Controller and a Data Processor, as defined by the legislation.

Personal data is defined as, data relating to a living individual who is an EU citizen and who can be identified from:
• That data;
• That data and other information which is in the possession of, or is likely to come into the possession of the Data Controller and includes an 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.

Sensitive personal data is defined as personal data consisting of information as to:
• Racial or ethnic origin;
• Political opinion;
• Religious or other beliefs;
• Trade union membership;
• Physical or mental health or condition;
• Sexual life;
• Criminal proceedings or convictions;
• Data that may be used for identity theft or fraud.

In summary, sensitive personal data is that which may cause harm to an individual if disclosed, stolen or otherwise misused, accidentally or otherwise.

Handling of personal/sensitive information

The Community Council will, through appropriate management and the use of criteria and controls:

• Observe fully conditions regarding the fair collection and use of personal information;
• Meet its legal obligations to specify the purpose for which information is used;
• Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
• Ensure the quality and accuracy of information used;
• Apply checks to determine the length of time information is held;
• Take appropriate measures to safeguard personal information;
• Ensure that the rights of people about whom the information is held can be fully exercised under the legislation.

These include:

• The right to be informed that processing is being undertaken;
• The right of access to one's personal information within the statutory limit (40 days until 24 May 2018, thereafter 30 days);
• The right to correct, rectify, block or erase information regarded as wrong information;
• The right to forget individual personal data upon request after 25 May 2018.

Implementation

The Clerk of Campbell Park Community Council is responsible for ensuring adherence with the Data Protection legislation, with the assistance and support of the Lead Member for data.

Privacy by design

All projects and routine activities that involve processing personal data shall follow the Privacy by Design methodology as defined by the Information Commissioners Office. This includes, but is not limited to, the website, all emails both inbound and outbound, staff employment and health details, all resident data, all incoming enquires residents or otherwise, and all printed material such as the newsletter. A large element of this requirement is the correct and secure handling of data stored in Information Systems, however hard copy records must also be physically protected in secure areas.

Training

All staff and councillors must consent to undergo data protection and privacy awareness training within one month of employment or joining Council. A training record will be signed upon completion of the training and kept as long as the person remains in employment or a member of Council. Failure to undergo training may lead to email and other communication services being suspended until training is completed.

Online service providers

All online service providers must have a two-party Standard Clause Contract (SCC) in place where data storage location is either unknown or outside of the EU. This includes all email services, IT services, web services, cloud storage and data backup services. Failure to provide and execute an SCC will disqualify a service provider from use for any Council business. Councillors and staff will be trained not to use such disqualified services for any purpose, while conducting CPCC business. A list of qualified services will be maintained by the Clerk.

Reportable data breaches

A Data Protection Officer is appointed to make determinations regarding data breaches and to ensure that a comprehensive Privacy Impact Assessment is performed and kept up to date.

Data breaches may include staff or councillor activity that fails to follow this policy.

Data breaches must be reported to the Information Commissioners Office within 72 hours of detection. This is solely a DPO responsibility and may not be influenced by staff or councillors in any way.

Subject access requests

Any staff member or councillor who receives a subject access request from an EU citizen, whether written or verbally communicated, must refer the request without delay to the Clerk. The EU citizen does not have to state "I am making a subject access request", so training given to all staff and councillors must include recognition of the various forms that such a request may take.

Right to forget

From 25 May 2018, any staff member or councillor who receives a "right to forget" request from an EU citizen, whether written or verbally communicated, must refer the request without delay to the Clerk. The training given to all staff and councillors must include recognition of the various forms that such a request may take.

Personal data accuracy and retention

Personal data may not be retained indefinitely. The data retention policy is stated in the CPPC IT Policy.

Personal data stored on mobile devices or portable storage

Personal data under the control of CPCC may only be stored on mobile devices or portable storage that are the property of CPCC and which have encryption and other security measures to fully protect it from accidental loss or theft. Security measures are explained more fully in the CPCC IT Policy. Failure to follow this policy may result in a reportable data breach, whether accidental loss

or theft occurs or not, if personal data is placed at risk, intentionally or otherwise.

Registration with the Information Commissioner

The UK Information Commissioner maintains a public register of Data Controllers. The Community Council is registered as such.
The Data Protection legislation requires every Data Controller that is storing and processing personal data, to notify and renew their registration, on an annual basis. Failure to do so is an enforceable matter.
The Data Protection Officer will review the Data Protection Register annually, prior to notification to the Information Commissioner.
Any changes to the register must be notified to the Information Commissioner, within 28 days.
To this end, any changes made between reviews will be brought to the attention of the Data Protection Officer immediately.

Adopted:

Appendix 1 – Website and Cookies

The Community Council will

1. Fully comply with the PECR for cookie notification and management on the CPCC website and any other websites that CPCC may become responsible for providing as a service.

2. Provide a comprehensive Privacy Policy on the website detailing all data collection, storage and processing activity for residents, staff and councillors. This will be based on the ICO example.

3. Seek the *consent of each visitor to their website before a cookie is saved to the visitor's computer or mobile device, at the first visit.

4. Each cookie will be identified in the website Privacy Policy and its purpose explained.

5. Visitors, having previously accepted cookies, will be able to withdraw that consent at any time.

*It should be noted that cookies that are essential in order to make a site work are exempt from consent but not from being detailed in the Privacy Policy.