BROUGHTON AND BRETTON COMMUNITY COUNCIL

DATA PROTECTION AND INFORMATION SECURITY POLICY

PRINCIPLES & PURPOSE:

This Policy sets out the Council's commitment to information security within the Council and provides clear direction on responsibilities and procedures.

BROUGHTON AND BRETTON Community Council is a Data Controller, as defined under the Data Protection Act 1998, and has registered as such with the Information Commissioner's Office.

The Data Protection Act 1998 sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The Data Protection Act applies to anyone holding personal information about people, electronically or on paper.

As a local authority, the Council has a number of procedures in place to ensure that it complies with The Data Protection Act 1998 when holding personal information.

When dealing with personal data, the Council staff and councillors must ensure that they adhere to Schedule 1 to the Data Protection Act which lists the data protection principles in the following terms:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
  (a) at least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met; and
  (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act 1998 is also met.
- Personal data 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.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data 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 data subjects in relation to the processing of personal data.

Storing and accessing data
The Council recognises its responsibility to be open with people when taking personal details from them. This means that councillors and staff must be honest about why they want a particular piece of personal information. If, for example, a member of the public gives their phone number to staff or a member of the Council, this will only be used for the purpose it has been given and will not be disclosed to anyone else without their permission.

The Council may hold personal information about individuals such as their addresses and telephone numbers. These will be securely kept at the Council Office and not available for public access.

All data stored on the Council Office computers is password protected. Once data is no longer required, or is out of date it will be shredded or securely deleted from the computer.

People have the right to access any personal information that is held about them. If a person requests to see any data that is being held about them

- They must be sent all of the personal information that is being held about them
- There must be an explanation for why it has been stored
- There must be a list of who has seen it
- It must be sent within 40 days

A fee to cover photocopying and postage charges may be charged to the person requesting the personal information.

Disclosure of personal information
If an elected member of the council, for example a Councillor, needs to access information to help carry out their duties, this is acceptable. They are only able to access as much information as necessary and it should only be used for that specific purpose. If, for instance, someone has made a complaint about over hanging bushes in a garden, a Councillor may access an address and telephone number of the person who has made the complaint so they can help with the enquiry. A Councillor may only do this providing they represent the area that the subject lives in. However, before they access any sensitive information about a person, they would need consent to do this from the Clerk. Data should never be used for political reasons unless the data subjects have consented.

Confidentiality
The Councillors and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

PROTOCOLS
System Security Processes and Procedures
The Council will provide and maintain security processes and procedures for all key information systems'. The procedures will uphold the principles of confidentiality, integrity, availability and suitability and be assessed for their impact upon other systems and services.

The security procedures will provide preventative measures to reduce the risks to the system, the information held within the system and the service it supports.

A Continuity plan will be developed and maintained for each system to ensure the principles are sustained and enable the continuation of services following failure or damage to systems or facilities.

The Clerk will be responsible for the implementation and promotion of the procedures.

Physical Security
Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms should be secured at all times with locked doors as a minimum security requirement.

All documents disclosing identifiable information will be transported in sealed containers eg envelopes.
Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, should not be left unattended or unsecured and paper records should not be left in public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment.

Logical Security
All computerised information and systems must be regularly backed up to a secure environment.

All computerised information systems will be password controlled and all passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person. All sensitive data will be password protected.

Copyright and licences
The Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the licence agreement.

Disposal and movement of equipment and media
Any media or IT equipment disposed of by the Council will not contain any data or codes that could allow an individual to be identified from it. The disposal of equipment will be made under a controlled and documented environment satisfying the requirements of the Data Protection Act 1998. The disposal of media such as disks and memory sticks must ensure that data cannot be recovered. Disposal of such media through the "everyday" waste collection is not permitted. The Council will implement processes to ensure appropriate disposal of such media.

An inventory of all Council computer equipment will be maintained. Details of any equipment or media disposed of or relocated (other than portable equipment) must be recorded.

Personal Computers
Computer users have responsibility for the security of the equipment in their care and shall not commit an act to compromise the data or Information Security Policy.

Computer users will be made aware of their responsibilities through this policy

Staff and Councillors' Responsibilities
The Council will make every reasonable effort to ensure that staff and councillors are aware of their responsibilities for the security of information and receive a copy of the relevant policies. However, each councillor or member of staff is responsible for ensuring that Security Policy is adhered to and report any breaches of security.

Incident Reporting
Incidents affecting security must be reported to the Clerk as quickly as possible. If necessary an incident may need to be reported to the Information Commissioner's Office.

Adopted: 18th September 2018