DATA PROTECTION
POLICY
July 2018

Cramlington Town Council is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000. The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants or partners 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 Act.

Statement of Policy

In order to operate efficiently, The Town 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 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. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

- Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met
- 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
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Shall be accurate and where necessary, kept up to date
- Shall not be kept for longer than is necessary for that purpose or those purposes
- Shall be processed in accordance with the rights of data subjects under the Act
- Shall be kept secure i.e. protected by an appropriate degree of security

• 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 Act provides conditions for processing any personal data. It also makes a distinction between **personal data** and **'sensitive' personal data**.

Personal data is defined as, data relating to a living individual 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.

Handling of Personal/Sensitive Information

The Town Council will:

• 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 only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
• Ensure the quality of information used;
• Apply strict checks to determine the length of time information is held;
• Take appropriate technical and organisational security measures to safeguard personal information;
• Ensure that personal information is not transferred abroad without suitable safeguards;
• Ensure that the rights of people about whom the information is held can be fully exercised under the Act. These include:
- The right to be informed that processing is being undertaken

- The right of access to one's personal information within the statutory 40 days- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information regarded as wrong information

In addition, The Town Council will ensure that:

• There is someone with specific responsibility for data protection in the organisation
• Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice

• Everyone managing and handling personal information is appropriately trained to do so
• Everyone managing and handling personal information is appropriately supervised
• Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do
• Queries about handling personal information are promptly and courteously dealt with
• Methods of handling personal information are regularly assessed and evaluated
• Performance with handling personal information is regularly assessed and evaluated
• Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All Town Council employees will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

• Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
• Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
• Individual passwords should be such that they are not easily compromised.

<u>All contractors, consultants, partners or other servants or agents of the Council must:</u>

• Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm

• Allow data protection audits by the council of data held on its behalf (if requested)
• Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation

All or any contractors who are users of personal information supplied by the council will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the Council.

<u>Implementation</u>

The Town Clerk is the designated data protection officer and is responsible for ensuring that the Policy is implemented and also has responsibility for:

• The provision of data protection training, for staff within the Council
• For carrying out compliance checks to ensure adherence with the Data Protection Act

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Cramlington Town Council is registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by Cramlington Town Council are entitled to: Ask what information the Council holds about them and why.

- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the Council is meeting its data protection obligations.

If an individual contacts the Council requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Town Clerk at cramlingtontc@gmail.com. This request can also be made by letter by writing to:

Cramlington Town Council
Surveyors House
Cramlington
NE23 1DN

The Town Clerk will provide the relevant data without undue delay and at the latest, within one month of receiving the request. The Town Clerk will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Cramlington Town Council will disclose requested data. However, the Town Clerk will ensure the request is legitimate, seeking assurances where necessary.

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Consent

The Council will document what personal data it holds, where it came from and who it is shared with. The regulation stipulates that anyone councils hold information on must give their explicit and 'informed' consent for their data to be retained for a set period of time and processed, which means the individual must be made aware of how their information is protected, what it's used for, and what the risks are. **The Council will follow the ICO GDPR consent guidance**

The GDPR includes the following rights for individuals:

- Right to be informed: we must provide 'fair processing information';
- Right to Access: confirmation that their data is being processed; access to their personal data; and other supplementary information;
- Right to rectification: people can correct incorrect information;
- Right to erasure: that is to be forgotten;
- Right to restriction of processing: we can store but not process the data;
- Right to portability: to take and reuse their personal data across a range of services;
- Right to object;
- Right to decision making: people can object if a human is not in the loop on a decision about them.

Data breaches

Under GDPR a data breach must be reported within 72 hours unless the controller can demonstrate that it's unlikely to result in risk to data subjects.

If there's a serious risk to data subjects they must also be notified. The risk would be the likelihood of fraud, or extreme distress or embarrassment.

Encryption is a likely panacea for breach notification obligations. If all breached data is encrypted the controller would not normally need to report it.

Data Protection Impact Assessments

Data protection impact assessments (DPIA, also known as privacy impact assessments or PIAs) are the practical tool required by the GDPR to assist organisations in the risk assessment process. DPIAs are a tool for identifying, assessing and reducing the data protection risks of your project and identifying and evaluating privacy solutions.

A single DPIA can be carried out covering a set of similar processing operations that present similar high risks. DPIAs should be carried out when:

- The data processing might result in a high risk to the rights and freedoms of the individuals

MUST be carried out when:

- Large scale processing of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to their rights and freedoms
- Large scale processing of special categories of data (previously referred to as sensitive data)
- Using new technologies and the processing is likely to result in a high risk to rights and freedoms
- Automated processing, including profiling, that results in automated decisions having legal effects or similar significant impacts on the data subject.

- The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual (e.g. personalised targeted direct mailings), profiling is not the same as market research segmentation.
- Systematic monitoring of a publicly accessible area on a large scale (CCTV)