HOUGHTON REGIS TOWN COUNCIL

Data Protection Policy

Date of Approval:	28th September 2015
Date of Review:	25th November 2019
Date of Re-approval	20th July 2020

Based on NALC Legal Topic Note 38**,** Data Protection November 2018

1.0 Scope

This policy must be complied with fully by all members, staff, agents, partners and contractors of Houghton Regis Town Council who collect, keep, process or deal with personal data for or on behalf of Houghton Regis Town Council.

Houghton Regis Town Council supports the objectives of the Data Protection Act 2018 (the DPA) and the GDPR (which also forms part of UK law) and intends to conform to the requirements of the Act at all times.

Houghton Regis Town Council needs to collect and use certain types of information about people with whom it deals in order to operate. This includes information relating to current, past and previous employees, suppliers, residents and others with whom it communicates.

Houghton Regis Town Council, as a data controller, pays a data protection fee to the Information Commissioner's Office (ICO) under the Data Protection (Charges and Information) Regulations 2018.

2.0 The Data Protection Act 2018 (DPA)

The DPA establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal

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

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in a transparent manner in relation to the data subject;
2. Shall be obtained only for specified, explicit 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 be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
6. Shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Definition of the Act are

"Controller" means the natural of legal person which, alone or jointly with other, determines the purposes of and means of the processing of personal data;

"Data subject" means the identified or identifiable living individual to whom personal data relates;

Personal data is defined as any information relating to an identified or identifiable living individual;
Identifiable living individual mean a living individual who can be identified, directly or indirectly, in particular by reference to-

(a) an identifier such as a name, an identification number, location data or an online identifier, or
(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify 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;
- Processing of genetic data and or biometric data
- Sexual life or sexual orientation;

3.0 Implementation of the DPA

Through appropriate management Houghton Regis Town Council will:

- Ensure that data is collected and used fairly and lawfully;
- Process personal data only in order to meet operational needs or fulfill legal requirements;
- Take steps to ensure that personal data is up to date and accurate;
- Establish appropriate retention periods for personal data;
- Ensure that data subjects' rights can be appropriately exercised;
- Provide adequate security measures to protect personal data;
- Ensure that a nominated officer (Town Clerk) is responsible for data protection compliance and provides a point of contact for all data protection issues;
- Expect all of its employees and councillors to comply fully with this policy and the principles of the DPA. Deliberate beaches of this policy will be considered as gross misconduct. Individuals, as well as the Town Council, can be prosecuted for breaches of the Data Protection Act;
- Provide adequate training for all staff responsible for personal data;
- Ensure that everyone handling personal data knows where to find further guidance;
- Ensure that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly;
- Regularly review data protection procedures and guidelines within the organisation

4.0 Processing Personal Data

Personal data must be processed fairly and lawfully in accordance with the provisions of the DPA.

Personal data may only be processed for notified purposes as stated with the DPA.

Anyone with responsibility for holding or collecting data must ensure that data kept and processed about any data subject is accurate and up to date. All due skill and care must be taken. Data must not be excessive to need, and superfluous data must be destroyed or removed from the system.

Houghton Regis Town Council is responsible for ensuring compliance with this policy and nominates the Town Clerk to ensure compliance with the Act and ensure that members of staff are aware of the provisions of the Act. In this role, The Town Clerk will be known as the Data Protection Act Representative. The nomination of such a person shall not release other members of staff from compliance with this Act and this policy.

Any processing of sensitive data must comply with the special and more stringent rules set out in the DPA.

5.0 Security and Registration

Each member, member of staff and data holder are responsible for ensuring that data cannot be accessed by unauthorised personnel and to ensure that data cannot be tampered with, lost or damaged. All superfluous data must be disposed of in a secure manner.

The Information Commissioner enforces and oversees the DPA and the Freedom of Information Act 2000. The Information Commissioner keeps a register of all organisations which process data. The Council shall submit a notification to the Information Commissioner and pay the prescribed fee in accordance with legislative requirements currently in force, which will be dealt with by the Town Clerk. Members and staff must furnish the Town Clerk with any information requested for this purpose. Members and staff must notify the Town Clerk if, during the course of any years, this information changes, and the Town Clerk must update the register entry accordingly. Members may have to register personally with the Information Commissioner with respect to constituency or party records.

6.0 Agents, Partner Organisations and Contractors

If a contractor, partner organisation or agent is appointed or engaged to collect, hold, process or deal with personal data for or on behalf of the Council or if they will do so as part of the services they are providing to Council, the Town Clerk must confirm that the agent, partner organisation or contractor is able, willing and does comply with the DPA. There must be specific obligations in every such partnership agreement and contract requiring the partner/contractor to comply with the DPA.

7.0 Disclosure of Personal Data

Personal data will only be disclosed in accordance with the provisions of the DPA.

8.0 Rights of Data Subjects

A person about whom information is held is, subject to any exemptions applying, entitled to:

(a) be informed by the data controller as to whether any information is held on then along with;
  (i) a description of the data; and
  (ii) a copy of the information

(b) request and receive information giving:
  (i) the purposes for which the data is being held
  (ii) the recipients
  (iii) the source of the data

(c) restrict processing of their data

(d) object to the processing of personal data for direct marketing purposes

(e) not to be subject to automated decision-making

(f) receive compensation from the data controller and/or the data processor for the damage suffered as a result of an infringement of GDPR

(g) obtain from a data controller without undue delay the rectification of inaccurate personal data

(h) erase personal data

(i) be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights

(j) to receive a copy of personal data or to transfer personal data to another data controller (data portability)

Access to personal data held by a data controller must be dealt with within one month of request, free of charge. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the data controller may charge a fee for providing the information or refuse to respond.

9.0 Disclosure to and about Third Parties

Personal data must not be disclosed about a third party except in accordance with the DPA. If it appears absolutely necessary to disclose information about a third party to a person requesting data about themselves advice must be sought from the Data Protection Act Representative.

10. Inaccurate Data

If an individual complains that the data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime, a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

11. Requests by Individuals to Stop Processing Information

If data is properly held for communication purposes, an individual is entitled to require that this is ceased as soon as possible. Requests must be made in writing but generally all written or oral requests should be heeded as soon as they are made. The cessation must be confirmed in writing.

If data is held for any other purposes an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data is held in connection with a contract with the person, if the Council is fulfilling a legal requirement or if the person's vital interests are being protected. Valid written requests must be heeded within 21 days. The cessation must be confirmed in writing.

12. Complaints

Any complaint or concern expressed by an individual in connection with the DPA must be reported to the Town Clerk immediately in case legal action is taken. The Town Clerk will ensure that there has been no breach of the DPA and, if so, take the necessary remedial action.

13. Exemptions

There are a number of purposes which are exempt from certain provisions of the DPA. Clarification on the scope of exemptions can be sought from the Town Clerk.

14. Violations of Rules and Procedures

It is the responsibility of all members of staff to report any suspected breaches of the DPA, or of this policy, to the Town Clerk.

It is the responsibility of all members to report any suspected breaches of the DPA, or this policy, to the Town Clerk or the Deputy Town Clerk.

Failure to comply with this policy by employees of the Council may result in disciplinary action being taken. Failure to comply by members of the Council may constitute a breach of the Members' Code of Conduct. Failure to comply by partners, agents or contractors may constitute a breach of their agreements.

15. Further Information and Other Related Policies

If in doubt about any aspect of this policy, the Town Clerk should be consulted.

Other related policies include the Equal Opportunities Policy and the Freedom of Information Policy.

For more information on the Data Protection Act, the Information Commissioner's website provides useful guidance,
https://ico.org.uk/for-organisations/guide-to-data-protection/

This policy will be monitored and reviewed by Corporate Services Committee every 4 years or in response to changes in legislation