Data Protection Statement [to be acknowledged by staff and Councillors]

Data Protection Act.

The Data Protection Act and General Data Protection Regulations regulate the use of "personal data" by an organisation. Please refer to the Council's Data Protection Policy for further information.

Registration with the ICO

The Data Protection Act requires that every organisation processing personal information to register with the ICO, unless they are exempt. This is a publically available document which lists all organizations that process data.

The Clerk will be responsible for ensuring that the Council's registration is kept up to date and all fees to the Information Commissioner are paid on time. The annual registration renews each August.

Collecting Information and consent

The GDPR requires organizations to have a lawful basis for processing personal information.

(a) Consent: the individual has given clear consent for the Council to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the Council.

(c) Legal obligation: the processing is necessary for the Council to comply with the law.

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for the Council to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for the Council's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

<u>For existing business functions</u>

The GDPR requires organizations to be proactive in informing customers of the reasons and terms of processing their data. For existing data held, the Council needs to review existing consents and its consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

The Council is in the process of redesigning its application and subscription forms to contain a request for consent which is prominent and separate from our terms and conditions but most of its core functions are covered by processing for legitimate or contract purposes.

When collecting allotment dues, booking activities and events, responding to planning applications, granting permission to use Council land or property, licencing allotments there is a clear lawful basis for processing customer information and no additional action need be taken by the Clerk.

The Council offers a number of subscription emails and e-newsletters. Existing members of these subscriber lists will asked to confirm they still wish to hear from the Council before the GDPR comes into force in May 2018. A review of subscriber information will be carried out every three years and the invitation to opt in will be reissued. Users will also be able to unsubscribe from Council mailing lists at any time through the "unsubscribe" link contained at the footer of all e-communications.

For new projects or gaining consent for existing projects where consent for processing has not occurred

To satisfy the GDPR in "data protection by design", the Clerk should be advised of any new project or database and a privacy impact assessment should be completed.

Once the Council is satisfied that there is a lawful basis to process the personal information, the following steps should be taken in gaining consent.

It is the Council's responsibility to inform customers at the point of collection, the purpose for processing their data. If the Council asks customers for personal information it will:

- let them know why it is needed, where it is not obvious.
- only ask for the information that is needed and to make sure nobody has access to it who should not
- Seek permission and let customers know there is a need to share it with other organisations
- only keep it for as long as necessary.

In return, to keep information reliable and up to date customers and staff will be asked to:

- to provide accurate information
- to inform the Council as soon as possible of any changes, such as change of address

The GDPR sets a high standard for consent to process data and requires a positive opt-in and not any other pre-ticked boxes or any other method of default consent.

Consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service (for allotment fees).

The Council's communications should clearly inform people that they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means that there needs to be a simple and effective withdrawal mechanisms in place.

The Council must keep clear records to demonstrate consent. it also needs to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Data retention, storage and disposal.

Personal data will need to be retained for longer in some cases than in others. Some data must be kept for a defined period as set out by law, in the Limitation Act 1980. This would include information pertaining to contracts, staff personal files, tax records and any information used in a personal injury claim.

HR

- Recruitment information (applications for jobs) should be kept for one year and then securely destroyed using confidential waste
- Staff personal files should be destroyed six years after the date of leaving

Finance

- Financial information to include invoice, receipts, petty cash books, orders and delivery notes and contracts should be kept for seven years for tax purposes.

The majority of information collected by the Council does not fit in to these criteria. How long it retains different categories of personal data should be based on individual business needs. A judgement must be made about:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure it remains accurate and up to date.

It is good practice to regularly review the personal data held, and to delete anything no longer needed. Information that does not need to be accessed regularly, but which still needs to be retained, should be safely archived or put offline. Staff and Councillors should review the personal information they hold individually or as part of a working party annually.

Any personal information must be stored securely. Paper files should be kept in a locked drawer, filing cabinet or storage facility. Electronic files with names, addresses and non-sensitive data will be adequately protected on the Council's network.

There are very limited occasions whereby the Council would need to collect sensitive personal information (for example medical information). In almost all cases this will be for HR purposes and will be stored on secure cloud based software programmes with high levels of IT security. The case for holding any such information should be rigorously tested and approved by the Chairman in conjunction with the Clerk. Where it is agreed that there is a legitimate reason to process this data, files must have the highest levels of security applied, to include password or other encryption. Under no circumstances should this information be removed from the Council's Office and any such information which has no legitimate reason for processing must be destroyed securely immediately.

Children

The processing of the personal data of a child is lawful where the child is at least 16 years old. For children under 16 years old, consent from the parent or guardian must be sought.

Data requests – providing information

Anybody requiring data about themselves should be requested to write to the office detailing their request. Such requests, known as subject access requests (SARs), must be complete within 30 working days from date the written request is received. Therefore any SARs must be date marked and immediately forwarded to the Clerk for action. The Council can offer to forward any correspondence, or information, should its records show that it holds such data.

If the Council holds information it will

- give a description of it;
- tell the person why it is held;
- tell the person who it could be disclosed to; and
- provide them with a copy of the information held where they are entitled to it.

Of prime importance is that personal information is not given out recklessly. Therefore no information is to be given over the telephone to any person whatsoever and the Clerk should be advised of the subject access request within 24 hours. No charge can be made for the provision of this data.

Data Breaches

If anyone becomes aware that personal information has been lost, stolen or hacked they should contact the Clerk immediately, with as much detail as they have available and

including where possible the nature of the information and the individuals affected by the loss.

Information Commissioners Office must be notified of a breach within 72 hours of the Clerk becoming aware of it, even if all the details are not yet known. Records of any breaches will be kept, even if they don't need to be reported.

Officers or Councillors who have any queries on this Standing Order must seek further clarification.