City of Winchester Trust Data Protection Policy

This policy applies to the running of City of Winchester Trust. The policy sets out the requirements that we have to gather data for stakeholder (members, employees and volunteers) purposes. The policy details how data will be gathered, stored and managed in line with the General Data Protection Regulation (GDPR). The policy is reviewed on a regular basis to ensure that we are compliant. This policy should be read in tandem with our Privacy Policy.

This data protection policy ensures that we:

- Comply with data protection law and follow good practice.
- Protect the rights of stakeholders and partners.
- Are open about how we store and process stakeholders data.
- Protect ourselves from the risks of a data breach.

GENERAL GUIDELINES FOR COUNCIL MEMBERS

- Access to data covered by this policy will be limited to those who need to contact or provide a service to our stakeholders.
- We will provide training to Council members and future Council members to help them understand their responsibilities when handling personal data.
- We will keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords will be used on data and they will be never be shared if more than one person is to have access to the stakeholder data.
- Data will not be shared outside of our Trust unless with prior consent and/or for specific and agreed reasons.
- We will request help from Information Commissioners Office if we are unsure about any aspect of data protection.

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation identifies 8 data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data is correct and any inaccurate data is erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 8 - Personal data cannot be transferred to a country unless that country ensures an adequate level of protection for the rights of individuals in relation to the processing of personal data.

We request data from stakeholders so we can contact them about their involvement with our Trust. The forms used to request data contain a privacy statement as to why information is being requested and what it will be used for. Stakeholders will be asked to provide consent for their data to be held and a record of this consent and their data will be securely held. Stakeholders can, at any time, remove their consent by contacting the Membership Secretary. Once a Stakeholder requests not to receive certain contact this will be acted upon promptly and reported to them.

PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

Stakeholders will be told for what we use their data. Appropriate use of Member data will include:

Contacting stakeholders about our events and activities

Contacting stakeholders about their membership/employment/volunteering and/or renewal of their Consent.

Contacting stakeholders about specific issues that may have arisen during the course of their membership/employment/volunteering.

Occasionally we will send to stakeholders details of activities that other organisations are providing that the Council think will be of interest to our stakeholders

We will ensure inappropriate contact is not made to our stakeholders such as marketing and/or promotional materials from external service providers.

We will ensure that use of stakeholders' data does not infringe their rights which include:

The right to be informed.
The right of access.
The right to rectification.
The right to erasure.
The right to restrict processing.
The right to data portability.
The right to object.

Stakeholders will only be asked to provide data that is relevant for membership/employment/volunteering purposes. This will include:

Name.
Postal address.
Email address.
Telephone number.

Any further data will be obtained with the specific consent of the stakeholder who will be informed as to why this data is required. Any such data will be deleted once that event has taken place unless it was to be required – with agreement – for a longer period.
Where a stakeholders' data needs to be shared with a third party involving statutory authorities then consent does not have to be sought from the stakeholder.

We have a responsibility to ensure stakeholders' data is kept up to date. Stakeholders will be asked to let the Trust Secretary know if any of their data changes.

We will ensure that we are compliant with data protection requirements and can prove it. Stakeholders will be asked to provide consent which will be securely held as evidence of compliance. We will also stay up to date with guidance and practice of GDPR and will seek additional input from the Information Commissioners Office should any uncertainties arise. We will review data protection and what data is held and who has access to it on a regular basis.

The Council have contracted for services from with the following 3rd party data processors:

Website services
Local Printer to print our TrustNews and Annual Report & Accounts.

Bulk Email transmission service.

The Council has examined their Terms and Conditions and judge that they are GDPR compliant. In fact in the first two cases no stakeholder data is provided. The bulk email service simply receives a list of email addresses.

Stakeholders can request access to the data we hold on them by contacting the Trust Secretary and we will normally deal with a request within 14 days. A record will be kept of the date of the request and the date of the response.

Where a data breach has occurred action will be taken to minimise the harm. We will seek to rectify the cause of the breach as soon as possible. We will contact the Information Commissioners Office within 72 hours of the breach being reported. We will contact the relevant members to inform them of the data breach and actions taken to resolve it.

If a stakeholder contacts us feeling that there has been a breach, he/she will be asked to produce an email or a letter detailing their concern. We then will investigate the breach. The stakeholder will also be informed that he/she can report their concerns to the Information Commissioners Office. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: 03/20

City of Winchester Trust Council
May 2018 Draft