CRANLEIGH PARISH COUNCIL

Cranleigh Youth Council
Data Protection Policy
November 2017

The Data Protection Act 1998 governs the collection, recording, storage, use and disclosure of personal data, whether such data is held electronically or in manual form. Young people have the same rights as adults under the Act.

Contents

1. What is Data Protection?

Data protection aims to protect an individual's rights to privacy by regulating how organisations obtain, store and use their personal data. So, data protection rules provide individuals with certain rights whilst also imposing certain duties and obligations on organisations. Young people and adults have the same data protection rights under the law.

a) The Law and Regulation

Data protection is governed by the Data Protection Act 1998 - DPA which is overseen and regulated by the Information Commissioner's Office - ICO.

b) What records are subject to Data Protection?

The rules apply particularly to computer or automated records (including email) but also apply to manual records kept in such a way that specific information about a particular individual can easily be retrieved e.g. manual records filed by the name or role etc.

Examples of automated records include:

- Computer files - files stored on hard file or floppy discs, CD Roms, DVD's, hard disks, back-up files
- Audio/Video-CCTV, webcam images
- Digitalised images- scanned photos, digital camera
- Examples of manual records include:
  - Files on employees, volunteers, young people
  - Index systems names, addresses, other details
  - Microfiche records- containing personal data

A mere passing reference to an individual is not necessarily classed as personal data e.g. the Minutes of a meeting will not be considered personal data about those attending in general. However, if an individual was specifically discussed and is identifiable from such discussion in the Minutes, then the Minutes will be personal data about that individual.

2. What is Personal Data?

This is any information held about a living individual who can be identified from the information itself or other information also held. Names, addresses or specific roles are obvious ways of identifying individuals but they can also be identified in photos or CCTV images.

For Cranleigh Youth Council, Personal Data might include: Parental consent forms, photographs, minutes of Youth Council meetings.

There are special rules applying to 'Sensitive Personal Data' where extra care must be taken when handling or disclosing it to third parties. Personal data becomes sensitive if it includes information about:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs;
- Trade union membership;
- Physical or mental health; or
- Sexual life;
- Commission of offences or alleged offences.

3. What are the rules?

The law states that when processing any personal data the Data Controller must apply 8 basic Data Protection Principles.

a) What is 'Processing'?

Processing has a wide meaning and includes all aspects of handling personal data e.g. from obtaining, recording, retaining (incl. editing and revising it), storing, sharing it to archiving and destroying it.

b) What is a Data Controller?

A Data Controller can be either individuals, organisations or other incorporated or unincorporated bodies of persons who determine what personal data is held, why it is held and how it is processed.

Data Controllers are responsible for ensuring compliance with data protection. At Cranleigh Parish Council, the Data Controller is the Proper Officer.

The DPA also refers to a data processor who processes personal data on behalf of the data controller, and for the Youth Council, the data processor will be the Councillor that collects and holds the parental consent forms including emergency contact details for members and the Proper Officer.

As the Data Controller is ultimately responsible for what the data processor does with the data, there should be a proper agreement specifying the Data Controller's instructions for the handling of the parental consent forms.

Youth Council Data

- When the parental consent forms are not in use at a meeting or outing of the Youth Council, they should be stored in the locked personnel filing cabinet in the Council Offices.
- Minutes of Youth Council meetings should be kept in a designated file and stored in the locked personnel filing cabinet in the Council Offices.

- Electronic copies of photographs of the Youth Council should be held on the secure area of the Council's server and hard copies stored in the locked personnel filing cabinet in the Council Offices.

c) What are the 8 basic principles of the DPA?

The 8 basic principles address fairness, lawfulness, relevance, excessiveness, accuracy, up-to-datedness and security. Thus, when processing personal data, the Data Controller must ensure that the data is:

- Processed fairly and lawfully;
- Obtained for a specified and lawful purpose;
- Adequate, relevant and not excessive for purpose;
- Accurate and up-to-date;
- Kept only for as long as required;
- Processed in accordance with the data subjects rights;
- Be kept secure proportionately to the level of harm that could result if unauthorised access occurs;
- Not transmitted outside the European Economic Area (EEA) without consent from the data subject.

4. How does Data Protection apply to the Youth Council?

4.1. Does data protection apply to the Youth Council?

Data protection law applies in full to the Youth Council as it collects and stores personal data about Youth Council members.

a) Does the Youth Council have to register with the ICO?

No as the Parish Council is registered as a Data Controller with the ICO and the Youth Council operates with a constitution agreed with the Parish Council.

b) Who within the Youth Council is responsible for Data Protection?

All Councillors at each meeting or outing will be the designated data processor and responsible for collecting and holding parental consent forms including emergency contact details for members.

c) How could Data Protection impact the Youth Council?

- The processing of personal data.
- When individuals make a 'Subject Access Request' ('SAR') i.e. a request for disclosure of all their personal data.

5. How Personal Data must be processed

The Youth Council must apply the 8 basic Data Protection Principles when processing Personal Data and the following are some basic essentials to be applied:

(a) When obtaining Personal Data

- have legitimate grounds for collecting and using it in the first place.
- be transparent about the purpose for which it is collected and who it will or may be shared with by providing privacy notices when collecting it.
- ensure you have consent from the individual.
- ensure that the source is clear.

(b) When retaining Personal Data

- only hold and retain data sufficient for the intended purpose.
- take reasonable steps to ensure accuracy as to facts and consider any challenges to this
- update, edit and revise it regularly in accordance with the purpose it was collected, e.g. changes to names, addresses, contact details, medical needs etc.
- review how long it should be retained in accordance with the purpose it was collected.
- give individuals access to their personal data.

(c) When storing Personal Data

- ensure secure system policies of storage, including encryption where necessary, and access in order to prevent accidental loss, alteration or breaches of security.
- be clear about who is responsible for ensuring information security.
- swiftly and effectively respond to any breach of security including reporting this to the ICO.

(d) When sharing Personal Data

- personal data must always be processed fairly, handled for intended purpose and only in ways that an individual would reasonably expect. This means that a data controller should not share personal data without legitimate reason.

(e) When deleting, destroying or archiving Personal Data

- Delete or destroy when no longer required securely.
- Archive securely where retention is justified.

(f) What are the special rules for processing 'Sensitive Personal Data'?

- All the above rules are also applicable when processing sensitive personal data but an additional rule applies to sensitive personal data which may only be held with the explicit consent of the data subject i.e. where sensitive personal data is to be processed, you must ensure that individuals have given explicit consent for this to happen. The DPA does not define the method of obtaining explicit consent, however, the best method is to obtain such consent in writing requiring the individual to e.g. tick a box or sign a declaration etc, agreeing that their sensitive personal data may be processed.

(g) Data controllers must not:

- Use personal data in ways which have an unjustifiable adverse effect on the individual.
- Transfer personal data to a country or territory outside the European Economic Area (EEA) unless first ensuring that country or territory also ensures a like level of protection for the processing of personal data.

6. How to deal with Subject Access Requests (SARs)

(a) What is an SAR?

One of the main rights which the Data Protection Act gives to individuals is the right to access their personal information. An individual can make a request in writing to an organisation for a copy of any personal information held about them. This is known as a Subject Access Request (SAR).

Following a request, a data subject is entitled to a copy of personal data being held or being processed about them (with only a few exemptions possible). The data controller may charge a standard fee to the data subject (a maximum of £10).

You must comply with the SAR within 40 calendar days of receiving payment.

(b) What can the Subject do following receipt of their Personal Data?

Subjects can:

- ask to have inaccurate data rectified, erased or destroyed.
- ask that data be stopped from being processed if it is unnecessary or causing unjustified damage or distress.
- ask the ICO whether the Act has been contravened.
- If necessary, apply to court to exercise their rights and may receive compensation if damages are suffered due to any contravention of the Act.

Review: February 2021