EVESHAM & DISTRICT u3a – PERSONAL INFORMATION AND DATA PROTECTION POLICY

Definitions

Personal Information: Anything in recorded form that says something about an identifiable individual.

Personal data: Personal information about a living individual held in or produced by electronic means or held in a filing system.

Policy

Evesham and District u3a will take all necessary steps to ensure that all personal information it handles (whether or not held as data) is treated with due regard to the privacy expected by the subjects of that information.

To this end we will:

1.Produce and regularly review a Privacy Notice

This will explain:

- our contact details;
- the types of personal information we collect;
- where we get this from;
- why we have people's information and what we are doing with it;
- the lawful basis for handling it;
- who we share personal information with;

- how long we hols personal information foe before getting rid of it, and;
- how to complain.

2.Retain personal information safely

Taking into account the privacy that individuals would expect, personal information, however held, will be kept safe. The level of security will be dependent on the sensitivity of the information.

As technology changes so rapidly, this policy itself contains no specific security requirements. If the sensitivity of the information requires it, consideration will be given, for example, to: secure electronic storage, access only by strong password, restricted access, secure document containers, keeping papers in a locked cabinet.

3.Take care to avoid unwarranted disclosure

In particular, care will be taken with electronic communications to ensure that they do not disclose personal information, including email addresses, to anyone who should not receive it.

4.Take special care with sensitive material

If the Grievance or Disciplinary procedures are invoked, we may have to handle very sensitive and confidential material. Sensitive personal information requires higher standards of care and security. Appendix 2 to this Policy provides guidance on document handling for these procedures.

5.Use personal information properly

Personal information we hold will be used only for the purposes for which it was provided or for other purposes that are legally permitted or expected.

6.Destroy personal information when no longer needed

Once it is no longer needed, personal information will be destroyed. Electronic information should be effectively deleted. Information on paper should be destroyed in a manner that leaves it unreadable. Some personal information e.g. in Minutes, newsletters, webpages, may be archived.

7.Remind all those handling personal information of their responsibilities

Committee members, group leaders and individual members will be reminded of their responsibilities when handling personal information on our behalf. Reminders will be issued by direct communication and through the website, newsletter or meetings when required.

8.Handover records on change of roles

Where an individual, because of the role they hold in the Branch, has had access to personal information for which the Branch is responsible, on ceasing to hold that role, their access to that information will discontinue. Any paper records will be handed over or destroyed, whichever is required.

Appendix 1

Breach Procedures

i) Complaint

The Privacy Notice will include a section on how to complain. Where a complaint is received, it will be investigated by members of the Committee who are not in any way implicated by it. Where the Committee needs support, or if the breach is serious, National Office will be notified. If the complainant is a u3a member, they will be informed that they can report their concerns to National Office if they are dissatisfied with the response from the Committee. Complaints will be subject to a full investigation, records will be kept and all those involved will be notified of the outcome.

ii) No complaint

Where a possible breach comes to the attention of the Committee other than on complaint, the matter will be investigated as if a complaint had been made.

iii) Action

Where it is concluded that a breach has occurred and an individual's privacy has been compromised, the Chair will notify National Office forthwith and will seek advice.

All Committee Members will be made aware that a breach has taken place

and how the breach occurred. The Committee will then seek to rectify the cause of the breach as soon as possible and take steps to prevent further breaches. Action will be taken to minimise any harm done.

Where the breach has come to light other than by complaint, the Committee will contact the relevant individual(s) to inform them of the breach and the actions taken to resolve it.

The Information Commissioner's Office will be notified of a breach involving serious risk to an individual.

iv) Retention of Records

A single record made under these procedures will be retained by the Branch Secretary (current and subsequent) for three years after the conclusion of investigation and then destroyed. All other copies will be destroyed at the conclusion of the investigation.

Appendix 2

Breach Procedures

It goes without saying that investigations into Grievances or Disciplinary matters must be carried out with absolute confidentiality. Not only is this good practice but, when documentation is produced, the requirements of the General Data Protection Regulations come into play. Some allegations may involve information that is sensitive personal information, which will require higher standards of care and security.

a)Disclosure

Do not disclose anything about the investigation with anyone other than those directly involved in it. Take great care to avoid accidental disclosure.

b)Secure Storage

Sensitive personal information should always be kept in secure conditions. Paperwork should be kept, for example, in a locked filing cabinetor locked drawer. If the material is kept with other routine information in the home, it should be placed in a folder marked confidential and kept secure from other family members.

If you use your own personal electronic device to handle sensitive personal information, it must have up to date virus protection. If the device is shared with other family members, the material must be filed in a password protected folder.

c)Secure transmission

Great care should be taken when sensitive information is being sent to other members of the Committee or those involved in an investigation. Secure means of communication should be used sand care taken to address the information correctly and mark it confidential.

In general, e-mail is not a very secure method of communication and should not be used to transfer sensitive personal information.

d)Secure disposal

Once a Grievance or Disciplinary matter has been concluded, one copy of the paperwork will be retained by the Branch Secretary, in secure storage, for 5 years and then destroyed. All other documentation generated by the procedure will be destroyed. Material on paper should be shredded, but if a shredder is not available it must be destroyed in amanner that leaves it totally illegible. Electronically held documents will be effectively deleted.

e)Special categories of Personal Information

If any matter under investigation includes information about:

- a person's racial or ethnic origin
- a person's health
- a person's religious or philosophical beliefs
- a persons sex life
- a person's sexual orientation
- a person's criminal behaviour

- terms that re widely defined – those carrying out the investigation need

to be aware of the additional restrictions on handling it. In the GDPR these are treated as special categories of personal information wioth additional handling restrictions. IN these circumstances, it may be necessary to have a document handling plan specific to the matter under investigation.

This Policy was approved on 18th March 2024
Review date: March 2027