Data Protection Policy

Data protection principles

Cambridge Council for Voluntary Service (CCVS) is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR) and other relevant legislation.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. 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.

General provisions

a. This policy applies to all personal data processed by CCVS, as well as other data kept in order to facilitate the running of the charity.

b. The Responsible Person shall take responsibility for CCVS's ongoing compliance with this policy. The responsible person is the CEO acting on behalf of the trustee board.

c. This policy shall be reviewed at least every two years.

Date Agreed July 2022

Review date July 2024

Personal Information and the rights of data subjects

A Data Subject is a person whose data is collected and used.

Personal information as referred to in this policy is any information relating to the Data Subject that is:

- Owned by them
- About them
- Directed towards them
- Sent/posted by them
- Experienced by them
- Relevant to them

People have a right to:

- understand what data organisations have about them and how it is being used
- see that information and get their own copy of it to use however they want
- correct the information if it is wrong
- ask for it to be deleted or limit how it is used
- complain if they don't like things an organisation is doing with their data.

Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.

b. The Register of Systems shall be reviewed at least every 2 years.

c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

Lawful purposes

All personal data processed by CCVS must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate.

a. CCVS shall note the appropriate lawful basis in the Register of Systems.

b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

c. Where communications are sent to individuals based on their consent, the option for the individual to revoke or unsubscribe their consent should be clearly available and systems should be in place to ensure such revocation or unsubscription is reflected accurately in the relevant systems.

Date Agreed July 2022

Review date July 2024

5. Data minimisation

a. CCVS shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

b. CCVS shall ensure that other data kept by the charity is only collected in order to ensure its proper running.

6. Accuracy

a. CCVS shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

c. CCVS will ensure that non personal data is correct and up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, CCVS shall put in place a procedure for each area in which personal data is processed and review this process every 2 years.

b. The archiving policy shall consider what data should/must be retained, for how long, and why. (see data register)

8. Security

a. CCVS shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, CCVS shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website). See appendix 2 for the data breach procedure.

END OF POLICY

Date Agreed July 2022

Review date July 2024

Appendix 1

Retention periods for key information

Document type	*Required retention period*
Accounting records	6 years after the end of the financial year to which they relate
Annual accounts and review	Permanently
Income tax and NI returns, tax records, correspondence with Inland Revenue	6 years after the end of the financial year to which they relate
Wage / salary records	6 years plus current year
Expense accounts and time sheets	6 years plus current year
Insurance Policies	Three years after lapse
Insurance Claims correspondence and Accident reports and relevant correspondence	Three years after settlement
Statutory Sick Pay records	6 years after the end of the tax year to which they relate
Statutory Maternity Pay records	6 years after the end of the tax year in which the maternity period ends
Accident books	3 years after the date of the last entry
Application forms and interview notes (for unsuccessful applicants)	6 months for unsuccessful applicants. For successful applicants all information will pass to their staff files.
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Statutory Maternity Pay records, calculations, certificates or other medical evidence	Three years after the end of the tax year in which maternity period ends
Statutory Sick Pay records, calculations, certificates, self-certificates	Three years after the end of each tax year for Statutory Sick Pay purposes
Trustees meeting minutes/AGM meeting minutes	Permanently for historical purposes

Date Agreed July 2022

Review date July 2024

Trustee details	6 years after the end of their service.
Supported volunteer information	3 years after last contact.
Newsletter sign up information	10 year
Support/enquiry contact information	5 years
Training course or event attendee information	2 years
Survey data with identifiers	2 years (after which all personal information will be removed and other data retained)
Membership information	5 years after ending of membership

Date Agreed July 2022

Review date July 2024

Introduction

This procedure sets out what CCVS will do in the event of a breach as well as the responsibility of all staff, trustees and volunteers when it comes to handing, storing and using personal data. Much of this comes from the NICVA GDPR toolkit. This can be found here www.nicva.org/data-protection-toolkit/

All staff and volunteers will be asked to sign that they have read and understood the data protection policy, these procedures and any accompanying documents.

What is a personal data breach?

The UK Information Commissioner's Office (ICO) defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

They highlight that "personal data breaches" can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an unintended recipient;
- Lost or stolen computing devices containing personal data;
- Unauthorised alteration of personal data; and
- Loss of availability of personal data.

If you are unsure if a breach has happened inform the CEO immediately and let them determine the way forward. Simply if in doubt, assume there was a breach.

A data breach does not just mean the loss of data, you may have sent information to the wrong person, you may have had a laptop stolen. It could be as simple as having some papers stolen that contain information.

How much time do we have to report a breach?

We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

It is essential that you inform the CEO of a breach (or potential breach) immediately you become aware of it.

Section II of the WP29 Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach.

If in doubt assume it is a reportable breach and inform the CEO.

Date Agreed July 2022

Review date July 2024

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When reporting the breach ensure you are able to pass on as much of this information as possible and be prepared to make obtaining the information your work priority. Do not delay reporting the breach because you do not have the information, report it anyway.

What happens after a breach?

The CEO will decide if the breach needs to be reported.

Both the identifier and the CEO will keep notes of what has happened and what actions have been taken.

The CEO will report the breach to the ICO if necessary.

The CEO will inform you if there is a need to contact the subjects of the breach, and will arrange for this to happen.

The CEO will inform the trustees.

A file will be set up on the hard drive to house all notes and copies of emails about data breaches regardless of the need to inform the ICO.

The CEO will deal with the ICO and any feedback from them.

Do we need to report to the ICO?

Not all breaches need to be reported to the ICO, but if the breach is likely to involve a 'risk to people's rights and freedoms', it must be (Article 33).

Such a risk would be one where the people involved could suffer adverse effects as a result of the breach. This depends on what was in the data and how it might be used to damage them, as well as

the scale of the breach. The inappropriate disclosure of sensitive or confidential information could be reportable if it would have a negative impact on someone's sense of privacy. Identify theft, fraud, financial loss and damage to reputation are other risks to rights and freedoms that could result.

The context, scale and level of sensitivity are more important than the nature of the breach. The same type of breach could be reportable or not, depending on the likely effect on individuals[1].

The CEO will assess the likelihood and severity of risks in deciding whether to report.

The CEO will note any conclusions and keep clear notes for the reasons for any decisions.

What do we need to tell the affected people?

There is a requirement in the GDPR to inform individuals affected as soon as possible (Article 34). This will allow them to take precautions and protect themselves against any negative effects, such as identify fraud.

The requirement to inform individuals is slightly higher than the need to report to the ICO. Compared to a "likely risk to individuals' rights and freedoms", you need to inform people if there is a "high risk".

The CEO will decide if it is necessary to contact the individuals, they will start from the assumption that although thresholds are different if there is a need to report to the ICO then we will tell the individuals.

The CEO will keep records of all decisions as well as all contacts that are made and any responses.

If it is deemed essential to inform the individuals we will include

- what happened
- what personal information was involved
- what risks are likely or possible
- measures being taken or proposed to address the breach
- contact details where they can get more information

[1] For example, accidentally sending a bulk email to invite a small number of people to a community event using the 'to' and not the 'bcc' field is unlikely to be a reportable breach. But sending a similar email to a group of people who are receiving mental health counselling would be, as the context identifies health information about those people.

Date Agreed July 2022

Review date July 2024