Data Protection Policy

Designated person: Lucy Dossor

Last review: December 2023	Next review due: December 2024

Contents

Aims Of This Policy

Growing Sudley CIC needs to keep certain information on its employees, volunteers, service users and board members to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers employed staff, freelance staff, board members, volunteers, activity participants, community.

Definitions and the 8 principles

In line with the Data Protection Act 1998 principles, Growing Sudley CIC will ensure that personal data will:

- Be fairly and lawfully obtained and processed
- Be processed for specific and lawful purposes
- Be adequate, relevant and not excessive
- Be accurate
- Not be kept for longer than is necessary
- Be processed in accordance with the rights of data subjects
- Be secure
- Not be transferred to other countries without adequate protection

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.

Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span.

Types Of Information Processed

Growing Sudley CIC processes the following personal information:

- Information on applicants for posts and voluntary work, including references
- Staff information – contact details, bank account number, payroll information, supervision and appraisal notes
- Board Member Information - contact details and professional information
- Supporters – contact details
- Activity Participants – contact details, medical information and project documentation and evaluation
- Community Groups, Partners and Individuals – contact details
- Donors and Funders – contact information, bank details

Personal information is kept in the following forms:

- Paper and computer based documents
- Online banking

Groups of people within the organisation who will process personal information are:

- Staff
- Board Members
- Volunteers

Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of Growing Sudley CIC, this is the Board Members.

The governing body delegates tasks to the Designated Person named above (Data Controller). The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- registering with and notifying the Information Commissioner as required*

All staff, board members, volunteers or project partners who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

**Based on the Self-Assessment questionnaire, Growing Sudley CIC is currently exempt from registering with the Information Commissioner's Office.*

Policy Implementation

To meet our responsibilities, staff, volunteers, board members will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;

- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

Gathering and Checking Information

Before personal information is collected, we will consider:

- What details are necessary for the purpose
- How long the details should be kept for

We will inform people whose information is gathered about the following (usually by way of the form they are being asked to fill in):

- why the information is being gathered
- what the information will be used for
- who will have access to their information (including third parties)

Personal Sensitive Information

Personal sensitive information is information about ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions etc.

Personal sensitive information will not be used apart from the exact purpose for which permission was given. Consent will be sought prior to this information being used again for another purpose.

Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

Any unauthorised disclosure of personal data to a third party by a volunteer or Board Member may result in termination of the volunteer/Board Member agreement and could result in personal liability arising from the breach.

Subject Access Requirements

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the designated person named at the top of the page.

The following information will be required before access is granted:

- Full name and contact details of the person making the request

- their relationship with the organisation (former/ current member of staff, Board Member or other volunteer, participant
- Any other relevant information- e.g. timescales involved

We may also require proof of identity before access is granted. The following forms of ID will be required:

Photo ID such as passport or driving licence

Birth certificate and proof of address

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

GDPR and Privacy Policy

In line with General Data Processing Regulations of May 2018, Growing Sudley CIC has developed a privacy policy governing the use of personal data. This Data Protection Policy should be used in conjunction with the Privacy Policy.

Contact

Growing Sudley CIC has appointed a designated person to deal with any issues or complaints about Data Protection and Processing, and to oversee the usage and security of data within the organisation. This person is named at the top of the document and can be contacted here:

Lucy Dossor

Data Protection, Growing Sudley CIC

43 Penny Lane, Liverpool L18 1DE

growingsudley@gmail.com

Appendix 1: Information Commissioner's Office Training Checklist

Training checklist for small and medium sized organisations

Data Protection Act

High-profile security breaches have increased public concern about the handling of personal information. As some 80% of security incidents involve staff there is a clear need for all workers to have a basic understanding of the Data Protection Act 1998 (DPA).

We recognise that some organisations have limited resources to devote to staff training. This note outlines some of the practical implications of the Act and is intended as a basic training framework for general office staff in small and medium sized organisations. Under each heading is a ***non-exhaustive guide*** to the points that should be covered in any training. Staff with duties such as marketing, computer security and database management may need specialist training to make them aware of particular data protection requirements in their work area.

1 Keeping personal information secure

Do your staff know:

- To keep passwords secure – change regularly, no sharing?
- To lock / log off computers when away from their desks?
- To dispose of confidential paper waste securely by shredding?
- To prevent virus attacks by taking care when opening emails and attachments or visiting new websites?
- About working on a 'clear desk' basis - by securely storing hard copy personal information when it is not being used?
- That visitors should be signed in and out of the premises, or accompanied in areas normally restricted to staff?

Data Protection Training checklist for small and medium sized organisations 20160202
Version: *1.3*

- About positioning computer screens away from windows to prevent accidental disclosures of personal information?
- To encrypt personal information that is being taken out of the office if it would cause damage or distress if lost or stolen?
- To keep back-ups of information?

2 Meeting the reasonable expectations of customers and employees

Do your staff know:

- To collect only the personal information they need for a particular business purpose?
- To explain new or changed business purposes to customers and employees, and to obtain consent or provide an opt-out where appropriate?
- To update records promptly – for example, changes of address, marketing preferences?
- To delete personal information the business no longer requires?
- That they commit an offence if they release customer / employee records without your consent?
- About any workplace monitoring that may be in operation?

3 Disclosing customer personal information over the telephone

Do your staff know:

- To be aware that there are people who will try and trick them to give out personal information?

- That to prevent these disclosures they should carry out identity checks before giving out personal information to someone making an incoming call?
- To perform similar checks when making outgoing calls?
- About limiting the amount of personal information given out over the telephone and to follow up with written confirmation if necessary?

4 Registration (notification) under the Data Protection Act

Do your staff know:

- Whether the company has registered with the ICO or is relying on an exemption?
- That you need to monitor changes in business use of personal information, and notify the ICO if appropriate?

5 Handling requests from individuals for their personal information (subject access requests)

Do your staff know:

- That people have a right to have a copy of the personal information you hold?
- How to recognise a subject access request?
- Who to pass it to if it is not their responsibility to answer?
- That the company has a maximum of 40 days to respond?
- That the maximum fee that can be charged is £10?
- That they may need to check the identity of the requester?
- What to do if other people's information is contained in the proposed response?

Other considerations

Additional guidance is also available if you need further information on:

- Registration under the Data Protection Act: https://ico.org.uk/for-organisations/register/
- Getting it right - A brief guide to data protection for small businesses: https://ico.org.uk/media/for-organisations/documents/1559/getting_it_right_a_brief_guide_to_data_protection_for_smes.pdf
- Getting it right - Small business checklist: https://ico.org.uk/media/for-organisations/documents/1558/getting_it_right_-_how_to_comply_checklist.pdf
- Employment Practices Code – A Quick Guide: https://ico.org.uk/media/fororganisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf
- CCTV Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- Releasing information to prevent or detect crime: https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf
- Electronic mail marketing: https://ico.org.uk/for-organisations/marketing/
- Calling customers listed on the Telephone Preference Service: https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/telephone-marketing/
- Checklist for handling requests for personal information (subject access requests): https://ico.org.uk/media/for-organisations/documents/1599/subject-access-checklist.pdf

Useful contacts

Federation of Small Businesses
Sir Frank Whittle Way
Blackpool Business Park
Blackpool
FY4 2FE
Phone: 0808 20 20 888
www.fsb.org.uk

Department for Business, Innovation and Skills
1 Victoria Street London SW1H 0ET
Phone: 020 7215 5000
https://www.gov.uk/government/organisations/department-for-business-innovation-skills

More information

This checklist will be reviewed and considered from time to time.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of data protection, please Contact us: see our website www.ico.org.uk.