Data Protection Policy

2017

Data Protection Policy

Supporting policies

- IT and Information Security policy
- CCTV policy
- Code of Professional standards (Employee Handbook)
- Disciplinary policy (Employee Handbook)

Aims of the policy

The Organisation needs to keep certain information on its employees, volunteers, associates, trustees, service users and supporters 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 applies to all employees, casual workers, associates, volunteers and trustees and it applies to all personal data and sensitive personal data collected and processed by the Organisation in the conduct of its business, in electronic format in any medium and within structured paper filing systems either stored on site or remotely.

Definitions

Data is defined as 'personal' if it:

- identifies a person, whether by itself, or together with other information in the Organisation's possession, or is likely to come into its possession; and
- is about a living person and affects that person's privacy.

In line with the Data Protection Act 1998 principles the Organisation will ensure that personal data will:

- be obtained fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for a specific and lawful purpose;
- be adequate, relevant but not excessive;
- be accurate and kept up to date;
- not be held longer than necessary;
- be processed in accordance with the rights of data subjects;
- be subject to appropriate security measures;
- not to be transferred outside the European Economic Area (EEA).

The definition of 'processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based personal data as well as data kept electronically.

The Personal 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 as follows.

- 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 than 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 to 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

The name of the Data Controllers within the Organisation are Organic Enterprises Ltd and the Henry Doubleday Research Association (HDRA) Ltd. HDRA Ltd and Organic Enterprises Ltd are separate entities that are both registered individually with the Information Commissioner's Office (ICO) to process personal data in order to provide a voluntary service for the benefit of the national public as specified in the Organisation's constitution; administer membership records; to fundraise and promote the interests of the charity; to manage employees and volunteers and maintain the Organisation's accounts and records. Processing also includes the use of CCTV systems for both the prevention and investigation of crime.

The Organisation notifies and renews its notification on an annual basis as the law requires. Any interim changes are notified to the Information Commissioner within 28 days.

Personal data is processed for past, current and prospective:

- Employees/casual workers
- Volunteers
- Trustees
- Associates
- Members
- Supporters/Donors
- Complainants/enquirers
- Service users
- Project beneficiaries

- Funders
- Site Visitors
- Suppliers
- Advisors
- Representatives of other organisations
- Individuals captured by CCTV images

Groups of people who will process personal information are:

- Employees
- Casual workers
- Volunteers
- Associates
- Trustees
- Third party suppliers

Personal information is held either in paper based filing systems or stored electronically.

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 Garden Organic, this is the Council of Trustees.

The governing body delegates tasks to the 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;
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes.

Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action and even criminal prosecution. The ICO also has the power to serve a monetary penalty notice on a data controller for breach of the Act.

Andrea Jackson is the Organisation's Data Protection Officer (DPO) and is responsible for the implementation of this policy. Any queries on the contents of this policy or data protection in general should be directed to Andrea Jackson on ajackson@gardenorganic.org.uk.

All employees, casual workers, volunteers, associates and trustees who process personal information must ensure that they not only understand but also act in line with this policy and the data protection principles.

Employees who breach the data protection policy may be subject to disciplinary action up to and including dismissal. Breach of this policy by casual workers, volunteers, associates, Trustees or any other affiliate of the Organisation may result in agreements being terminated. It is also possible for individuals to be subject to a monetary penalty for the most serious contraventions of protecting personal data.

Policy Implementation

To meet data protection responsibilities all employees, casual workers, volunteers, associates and trustees will:

- familiarise themselves with this policy and the IT and Information security/CCTV policies and adhere to them at all times;
- ensure any personal data is collected in a fair and lawful way;
- make individuals aware of the intended use of their data at the point of collection either verbally, written or via direction to the relevant privacy notice;
- ensure that only the minimum amount of information needed is collected and used;
- ensure the information is kept up to date and accurate;
- review the length of time information is held and establish appropriate retention periods;
- ensure personal data that is no longer needed (in line with departmental retention guidelines) is disposed of effectively and securely;
- ensure personal data is kept securely;
- ensure the rights people have in relation to their personal data can be exercised including opt outs and cease processing requests;
- be mindful that individuals have the right to see their personal data (e.g. comments sent in emails) and not record comments or other data about individuals which they would not be comfortable in the individual seeing;
- inform the DPO in the event of any intended new purposes for processing personal data - no new purpose for processing data will take place until the ICO has been notified of the relevant new purpose and the data subjects have been informed, or in the case of sensitive data, their consent has been obtained;
- report any actual, near miss or suspected data breaches (either accidental or as a result of theft) immediately to the DPO for investigation.

The Organisation will ensure that:

- a nominated officer is responsible for data protection compliance that provides a point of contact for all data protection issues;
- everyone managing and handling personal information is appropriately trained and supported to do so;
- everyone handling personal data knows where to find further guidance;
- adequate security measures are in place to protect personal data;
- any disclosure of personal data will be in line with organisational procedures;
- queries about handling personal information are dealt with effectively and promptly;
- data protection procedures and guidelines within the Organisation are reviewed regularly.

Prohibited activities

The following activities are strictly prohibited:

- transferring personal data outside the European Economic Area (unless that country or territory can ensure a suitable level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data);

- using data obtained for one purpose for another supplemental purpose (e.g. using contact details for HR –related purposes for marketing purposes);

- disclosing personal data to a third party outside of the Organisation without the consent of the data subject (unless an exemption applies such as matters relating to taxation or pursuing criminal justice).

Training

Training and awareness raising about the Data Protection Act and how it is followed in this Organisation will take the following forms:

<u>On Induction:</u>

Employees/casual workers

This policy along with the IT and Information Security policy and CCTV policy are contained within the employee handbook which is issued to all new employees/casual workers on their first day. All employees/casual workers must sign to say they have read and understood the contents and agree to abide by it.

All new employees including casual workers, will be asked to complete the Organisation's data protection e-learning module, for which a certificate is issued and also read the Organisation's Information Security presentation.

Department heads or seniors will also conduct department specific data protection briefings and issue guidelines.

Trustees/admin and office based volunteers

All trustees and admin/office based volunteers are to be issued with a copy of the relevant policies and procedures relating to data protection and IT and Information Security and asked to sign and return a form with their agreement to comply. They will also be asked to complete the Organisation's data protection e learning module and read the Information Security presentation. Where relevant, a department specific data protection briefing will be conducted.

Non-admin and non-office based volunteers

All non admin/office based volunteers are to be issued with a copy of the relevant policies and procedures relating to data protection and asked to sign and return a form with their agreement to comply. They will also be asked to read the Information Security presentation.

Associates

All Associates are to be issued with a copy of the relevant policies and procedures relating to data protection and asked to sign and return a form with their agreement to comply.

Ongoing:

In order for data protection to remain a salient issue the following will be undertaken by the DPO:

- an annual reminder to all employees/casual workers re-referring them to the Organisation's data protection policy;
- regular emails highlighting DP news/hints and tips/issues/interesting facts;
- posters around the office – particularly in 'at risk' locations e.g. printers/filing cabinets.

Selected communications will also be sent to volunteers, associates and trustees where appropriate.

Data security

Keeping data properly secure is key in complying with the Data Protection Act 1998. 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:

- paper based personal information will be stored in lockable cupboards with restricted access to keys by authorised personnel only;
- following UK government Cyber Essentials to ensure safety and security of IT systems including boundary firewalls and internet gateways, secure configuration of hardware and software, password control, malware protection and appropriate patch management/software updates;
- implementation of a robust back up strategy;
- appropriate electronic storage of personal data with folder access given only to authorised personnel;
- any personal data transferred from one place to another or stored off site will be done in line with the Organisation's IT and Information Security policy;
- personal information will only be stored for as long as it is needed or required by statute and will be disposed of appropriately.

Please refer to the Organisation's IT and Information Security policy for further information and rules on security.

Any unauthorised disclosure of personal data to a third party by an employee or affiliate is considered a breach of this policy which may result in further action as previously outlined in the responsibilities section of this policy.

Subject Access requests

Anyone whose personal information is processed by the Organisation has the right to know:

- what information the Organisation holds and processes on them;
- how to gain access to this information;
- how to keep it up to date;
- what the Organisation are doing to comply with the Act.

Individuals 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 DPO Officer. The Organisation may require proof of identity before access is granted.

The Organisation 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.

The Organisation's privacy notice will include a contact address for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how the Organisation is processing their data or about the Organisation's handling of their request for information.

Employees and affiliates are aware that in the event of a Subject Access request being received by the Organisation, all corporate systems including emails may be searched and relevant content disclosed whether marked as personal or not.

Data Privacy Impact Assessments

Any new projects or systems that involve different ways of collecting or processing personal data will be referred to the DPO at the initial set up stage to determine the risks and impacts to the personal data and ensure privacy and data protection compliance is accounted for from the onset.

Policy Communication

<u>Internal</u>

This policy is given to all new employees and affiliates at the point of entry into the Organisation. It is also stored on the Organisation's SharePoint.

External

This policy and the Organisation's privacy notice will be communicated externally by publishing it on the Organisation's website.

Review

This policy will be reviewed and updated before the onset of GDPR in May 2018. Thereafter the policy will be reviewed at 2 yearly intervals to ensure it remains up to date and compliant with the law.

Agreement

This must be signed and returned to the HR department within 1 week of being issued.

I have read and understood the data protection policy and agree to adhere to its contents.

Name and position: .....

Signature: .....

Date: .....