The Advantage Foundation Ltd.

Data protection policy

Advantage needs to collect and use personal data about people including past, present and prospective clients in order to carry on its business and meet its clients' requirements effectively. We recognise that the lawful and correct treatment of personal data is very important to successful operations and to maintaining our clients' confidence in ourselves.

Any personal data which we collect, record or use in any way whether it is held on paper, on computer or other media will have appropriate safeguards applied to it to ensure that we comply with the Data Protection Act 1998 ("Act"). We fully endorse and adhere to the eight principles of Data Protection as set out in the Act. These principles state that personal data must be:-

1. fairly and lawfully processed
2. processed for specified and lawful purposes and not in any other way which would be incompatible with those purposes
3. adequate, relevant and not excessive
4. accurate and kept up to date
5. not kept for longer than is necessary
6. processed in line with the data subject's rights
7. kept secure
8. not transferred to a country which does not have adequate data protection laws.

We will not disclose information to any third party unless we believe it is lawful to do so.

In order to meet the requirements of the principles, we will:

1. observe the conditions regarding the fair collection and use of personal data
2. meet our obligations to specify the purposes for which personal data is used
3. collect and process appropriate personal data only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements
4. ensure the quality of personal data used
5. apply strict checks to determine the length of time personal data is held
6. ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act
7. take appropriate security measures to safeguard personal data
8. no detailed client information will be removed from premises on usb
9. ensure that personal data is not transferred abroad without suitable safeguards.
10. when we collect any personal data from the client, we will inform the client why we are collecting the clients data and what we intend to use it for.

Where we collect any sensitive data, we will take appropriate steps to ensure that we have explicit consent to hold, use and retain the information. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

We have a responsible marketing policy and do not give client details, or details of related individuals, to any other company outside Advantage. Clients may be contacted by our enterprise partners in relation to services that may be of interest to the client. If clients do not wish to be marketed in this way they can opt out at any time.

Under the Act, clients may request a copy of the information which we hold about them. We reserve the right to charge the maximum fee payable in terms of the Act for providing this information. If the details are inaccurate the client can ask us to amend them.

The Advantage Foundation Ltd.

Data Breach policy

Personal data breaches

The Advantage Foundation Ltd will make all reasonable endeavours to ensure that there are no personal data breaches.

When appropriate, we will report the data breach to the relevant parties within 72 hours.

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the company's information assets and / or reputation.

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored
- (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;
- human error;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

Any individual who accesses, uses or manages Company information is responsible for reporting data breach and information security incidents immediately to the Director / Project Manager.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

An Incident Report Form should be completed as part of the reporting process. All staff should be aware that any breach of Data Protection legislation may result in the Company's Disciplinary Procedures being instigated.

Evaluation and response

Once the initial incident is contained, the Director will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing
- security measures;
- whether methods of transmission are secure;
- sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for
- reacting to reported breaches of security.
- If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Board of Directors.

Policy Review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

This policy was last reviewed in Feb 2019. The policy was approved by The Advantage Foundation Ltd on Feb 2019.