Data protection Policy The Adnan Jaffery Educational Trust t/a One Degree

ONE DEGREE

Review date: March 2020

Introduction

1. ONE DEGREE needs to process information about employees, organisations and individuals who use our services
2. When we process information, we need to keep to the terms of the Data Protection Act 1998. In particular, we need to make sure that we process information in line with eight principles of data protection described in the Act. (The eight principles are listed at the bottom of page 2.)
3. The Data Protection Act sets limits on the way we collect, store and use information. The Act controls how:
4. We file information
    a. how we access information
    b. how we pass information on to other organisations and individuals; and
    c. how and when we destroy information we are storing.
5. The Act says that people have a right to access any information that we hold about them. This includes employees, ONE DEGREE members and people who use our services. The Act says that we have to respond to requests for access to information within 40 calendar days
6. The Act says that organisations that process information need to register with the Information Commissioner's Office. There are exceptions to this rule for some not-for-profit organisations. Under these exceptions, ONE DEGREE does not have to register with the Information Commissioner
7. One Degree information and communication worker will deal with day-to-day data protection issues. One Degree Trustee Board has overall responsibility for ensuring that ONE DEGREE works in line with the Data Protection Act
8. One Degree Trustee Board, ONE DEGREE staff and any others who process personal information on behalf of ONE DEGREE must comply with the principles of the Act. ONE DEGREE's responsibilities
9. ONE DEGREE wants to protect the right of individuals to privacy
10. We will respect the privacy of individuals when processing personal information
11. We will take appropriate measures to make sure that the data we hold is stored securely
12. One Degree Trustee Board has overall responsibility for making sure that ONE DEGREE meets the terms of the Data Protection Act
13. ONE DEGREE management staff have a responsibility to make sure that staff process information in line with the terms of the Act. Staff responsibilities
14. Staff are responsible for the security of the information they process
15. Staff must not pass on information to anyone who is not entitled to it
16. Staff should make sure that any information they give to ONE DEGREE about their employment is accurate and up to date. Right of access
17. ONE DEGREE employees, members, and people who use our services have the right to access personal information ONE DEGREE holds about them, whether in electronic or paper form

18. People who want to access information held about them should contact One Degree information and communication worker
19. More information about individuals' right of access is available in Appendix 2 The eight principles of data protection The Data Protection Act states that anyone who processes personal information must comply with eight principles. These state that information must be:
    a. Fairly and lawfully processed
    b. Processed for limited purposes
    c. Adequate, relevant and not excessive
    d. Accurate and up to date
    e. Not kept for longer than is necessary
    f. Processed in line with individuals' rights
    g. Secure
    h. Not transferred to other countries without adequate protection

Appendix 1

Being open about how we will use information that individuals/organisations give us

The Data Protection Act says that we need to explain to people how we will use the personal information they give us.

ONE DEGREE also desires to be clear about how we will use organisational information which is supplied.

The following statement is a general explanation of how ONE DEGREE will use information.

This statement should be included on all forms, surveys, questionnaires and other documents where we ask for personal information.

If we are collecting information for a purpose that isn't included in this statement, we should amend the statement to make our full purpose clear.

How we use the information you give us Information you give ONE DEGREE will be used by us and our agents to tell you about ONE DEGREE services, and to give you information on issues relevant to the voluntary sector in Westminster.

ONE DEGREE will communicate with you by telephone, letter, email, or in any other reasonable way. You can ask for a copy of the information we hold about you and your organisation, and if the information isn't accurate, you can ask us to correct it.

If you do not want to receive letters, emails and telephone calls from us in the future, please tell us in writing.

ONE DEGREE may pass on details of your organisation's postal address to other voluntary and community organisations, or to local statutory organisations. We will never pass your contact details on to salespeople, or to private organisations.

If you do not want us to pass on your organisation's postal address, please let us know in writing.

If you have any questions about how ONE DEGREE will use information about your organisation please phone.

Appendix 2

Dealing with disclosure The Data Protection Act gives people rights to access personal information that organisations hold about them.

This guidance explains what rights people have, and what are responsibilities are. People have the right to know if we process (collect, store and use) their personal information.

People can ask us to tell them:

i. What kinds of personal information we process
ii. How we use personal information
iii. Who we pass personal information on to, and in what circumstances
iv. People can also ask for a copy of the information records we hold about them, and for us to explain where we got our information from. If people want to get a copy of the information records we hold about them, they need to ask us in writing. We have to respond to written requests within 40 days.
v. An individual only has the right to see personal information we hold about them personally – no one can ask to see another person's information. If someone asks for a copy of their information record we need to check that they are the person the record is about. In some situations, by giving out information about one person, we may also give out information that makes other people personally identifiable. For example, our training records might show the names of everyone who attended a training course on a particular date. The Data Protection Act (Section 7, sub-sections 4-7) has special rules to say what should happen in these situations and we need to work in line with these rules.
vi. People can also ask in writing to be removed from our records, or to say how and when we can use the information we hold about them. For example, someone might choose not to receive emails from us, but might still want to receive One Degree newsletter. We need to deal with requests like this within 21 days. In general, all requests relating to the use, storing or deleting of records should be made in writing One Degree information and communication worker.

Appendix 3

Passing on information One Degree statement how we will use the information you give us explains that ONE DEGREE will, in some circumstances, pass on contact information for organisations and individuals:

i. Information you give ONE DEGREE will be used by us and our agents to tell you about ONE DEGREE services, and to give you information on issues relevant to the voluntary sector.
ii. ONE DEGREE will communicate with you by telephone, letter, email, or in any other reasonable way. You can ask for a copy of the information we hold about you and your organisation, and if the information isn't accurate, you can ask us to correct it. If you do not want to receive letters, emails and telephone calls from us in the future, please tell us in writing. Your organisation's name and the contact details you give us will be added to a

directory of voluntary and community groups. This directory may be accessible to the public, and to other voluntary organisations. If you do not want your organisation to be included in the directory, please tell us in writing.

iii. ONE DEGREE may pass on details of your organisation's postal address to other voluntary and community organisations, or to local statutory organisations. We will never pass your contact details on to salespeople, or to private organisations. If you do not want us to pass on your organisation's postal address, please let us know in writing.

General guidelines:

- ONE DEGREE may pass contact information on to agents employed by ONE DEGREE to carry out a particular task (for example, asking volunteers to contact people on our database by telephone)
- Information listed on the online directory is already considered to be in the public domain. Contact details listed on the online directory may be passed on individually, but not collectively
- ONE DEGREE may pass contact information for organisations, individually or collectively, to members of the public, to public sector organisations, and to voluntary sector organisations
- ONE DEGREE may not pass on contact information for organisations, individually or collectively, to private sector organisations wishing to sell services or goods
- ONE DEGREE may not pass on information about an individuals' use of ONE DEGREE services, without permission from that individual.

Appendix 4

Security Personal information relating to the involvement of individuals and organisations with ONE DEGREE is stored centrally on One Degree database.

This data is limited to contact information, details of individuals' use of ONE DEGREE services, and details of individuals' mailing subscriptions.

- Data stored on One Degree database is not considered sensitive.
- Access to the database must be limited to current ONE DEGREE staff and agents
- Sensitive personal data must not be stored on the database (sensitive data includes information about an individuals' ethnicity, religion, sexuality or health, for example)
- The database is backed-up manually on a weekly basis. Automatic back-ups are run daily. Personal information relating to the recruitment and employment of ONE DEGREE staff is stored securely in a locked personnel cabinet. This information is considered sensitive.
- Access to the personnel cabinet is limited to management staff
- The key for the personnel cabinet is stored in a locked drawer
- Before disposal, sensitive personnel documents are shredded

Appendix 5

Data protection law reform General Data Protection Regulation (GDPR) taking effect from 25 May 2018, the below eight principles are relevant to our organisation and fully complied with:

1. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
2. Personal data shall be processed in accordance with the rights of data subjects under this Act.
3. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
4. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix 6

Breaches of data

In the event of a potential, suspected or actual breach of data then the Chief Executive Officer at One Degree must be notified immediately. Corrective actions will then be agreed within the service order to minimise the breach, inform the appropriate persons and take any actions required to correct such breach/s and ensure a repeat cannot happen. Data subjects may need to be notified that their data has been compromised and given details of the breach, what steps One Degree has taken to mitigate the breach and any potential repercussions of the breach for the data subject.