CASE Data Privacy Policy for Volunteers and Consultants

Handling Personal Information

Policy & Procedure

Contents

1. Introduction

1.1 The Council for Advancement and Support of Education (CASE) collects and uses a wide range of information about individuals in order to carry out its functions and deliver its services. These people include our members, customers, and employees, and the information we hold about them is their personal data. If we fail to take adequate care of the personal data we deal with and it is lost, stolen, disclosed inappropriately or otherwise misused, this could have a serious impact on the individuals concerned ranging from distress to actual physical harm. Personal information is therefore a valuable asset, but also a liability if handled incorrectly.

1.2 This policy and procedure is therefore designed to ensure that personal information is handled securely, in particular its storage and transfer, to assist in complying with CASE's legal obligations.

1.3 For the purposes of this document the term "Information Asset Owner" refers to the senior director of information and membership systems, under the guidance of the chief operating officer, the data management committee, and the data privacy subcommittee.

2. Definition of personal information

2.1 Personal information or data is any information that relates to a living individual, who can be identified from the information, directly or indirectly.

2.2 In practice, this is likely to include a very wide range of data, including, but not limited to:

- Names, addresses and dates of birth
- Reference numbers, such as employee or national insurance numbers
- Personal financial information such as bank or credit card details
- Descriptive or biographical information regarding an individual
- Photographs or other images

2.3 The terms "personal information" and "personal data" are used throughout this policy and procedure and have the same meaning.

2.4 There are also special categories of personal information and we must be particularly careful when dealing with these. The special categories are personal information regarding:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data

- Health
- Sex life or sexual orientation

2.5 There are also specific requirements for information relating to criminal convictions and offences.

3. Legal background

3.1 Data Protection legislation sets out rules relating to the processing of personal data. Processing is defined as collecting, recording, storing and making any use of personal data, including its disclosure and disposal.

3.2 Data Protection legislation that appropriate technical or organizational measures must be used to protect against unauthorized or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data.

3.3 The consequences of not handling personal data correctly could have serious consequences for CASE, as administrative fines of up to €20,000,000 (approximately $22M USD) can be imposed for serious Data Protection breaches.

4. Policy statements

4.1 CASE is committed to processing personal information in accordance with the requirements of worldwide Data Protection legislation.

4.2 CASE views the proper handling of personal data as essential in delivering our services and maintaining the confidence of the people that we deal with.

4.3 Any personal data held by CASE which is not in the public domain will always be treated as being strictly confidential.

4.4 CASE will make maximum use of secure electronic methods to store and transfer personal data.

4.5 This policy is approved by, and has the full support of, CASE.

5. Scope

5.1 This policy and procedure applies to all personal data owned by CASE.

5.2 This policy and procedure applies to all volunteers, consultants and contractors working on CASE's behalf.

6. Responsibilities

6.1 Volunteers, consultants and contractors are responsible for:

- Protecting the personal information they process by adhering in full to this policy and procedure.

6.3 Breaches of this policy and procedure may lead to removal of access to personal information related to CASE members.

7. Secure storage of personal information

7.1 Paper records, portable devices and removable media containing personal information must be kept securely.

7.2 Storage of personal data in paper records should be minimized where possible. If paper records must be stored, they should be securely maintained in locked file cabinets with restricted access.

7.3 Personal data must not be left unattended where anyone can have access to it, such as on desks, window sills, corridors, printers and photocopying machines.

7.4 In the case of contractors, volunteers or other third parties, where CASE equipment is not being used, personal information belonging to CASE will be shared by a CASE employee in a secure location. This information must never be saved on a personal computer, portable device or a non-CASE database or network.

7.5 Personal data must never be uploaded/stored in cloud storage not provided by CASE. This includes, but is not limited to:

- Personal email accounts (such as Gmail, Hotmail)
- Dropbox
- Google Docs
- Slack

7.6 When personal information is displayed on computer screens used in a public area, it must not be visible to members of the public.

8. Retention of personal information

8.1 When it is no longer necessary to keep personal data, it should be deleted immediately.

8.2 Where a portable device is used for the purpose of collecting personal information, the information should only be kept on it for as long as is absolutely

necessary. The information should be saved on CASE's network at the earliest opportunity and deleted off the device.

8.3 Paper records containing personal information must be disposed of securely, by shredding or the use of the confidential waste service**.**

9. Breaches of security

9.1 These would include cases where personal data is lost or stolen, either in electronic or paper format. Other examples would include emailing personal data to an unintended recipient or accidentally placing personal data on a website.

9.2 All security breaches must be reported immediately to privacyofficer@case.org

9.3 Failure to report, or delay in reporting, security breaches can have potentially serious consequences for data subjects, staff, other individuals and CASE.

10. Ensuring equality of treatment

10.1 This policy and procedure must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

11. Agreement to abide by the policy and procedure

11.1 I have read the *CASE Data Privacy Policy for Volunteers and Consultants* and understand that I am bound by the requirements detailed within it.

_____

Name (please print)

_____ _____

Signature Date