Project Challenge Protection Policy with GDPR

Lorna Butterick Data Protection Lead lorna.butterick@Project Challenge.org.uk 01422 363644	**Jill Wilson** Project Challenge Board Chair Jill.wilson8@me.com 01422 354605
Tom Harnett tom.harnett@Project Challenge.org.uk Deputy Data Protection Lead 01422 363644	Roger Harvey rharvey@harveysofhalifax.co.uk Board Data Protection Lead 01422 331188
Version 4: 19th September 2024	**Next Review Due: September 2025**

Introduction

PROJECT CHALLENGE is a Data Controller under the Data Protection Act and the General Directive on Data Protection (GDPR), which means that it determines the purposes for which personal information will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

PROJECT CHALLENGE needs to keep certain information about its employees, service users, volunteers, students and other service users to allow it to monitor its performance, achievements and operate effectively. It is also necessary to process information so that staff can be recruited and paid, so that courses can be organised and various legal obligations to funding bodies and government complied with.

To comply with legislation, information must be collected and used fairly, stored securely and not disclosed to any person unlawfully. To do this, PROJECT CHALLENGE must comply with the principles set out in the Data Protection Act 1998 and the 2018 General Directive on Data Protection(GDPR). PROJECT CHALLENGE is also committed to meeting its legal requirements under the Freedom of Information Act 2000.

Information that is already in the public domain is exempt from the 1998 Act and GDPR.

This policy should be read in conjunction with the Freedom of Information Policy and the PROJECT CHALLENGE Document Retention policy. The policy also applies to provision delivered in partnership with other providers and for all service users/ learners/volunteers who receive training in the PROJECT CHALLENGE name.

Amendments to this policy will be made in the light of new requirements under the General Data Protection Regulation (GDPR) being introduced from May 2018.

Project Challenge Protection Policy with GDPR

2. Policy Statement

PROJECT CHALLENGE will ensure that all personal data is processed fairly and lawfully, including under the new requirements of GDPR.

Any member of staff or service user who considers that this policy has not been followed in respect of personal data about themselves, should raise the matter with the appointed Data Protection Controllers initially. PROJECT CHALLENGE has a nominated Data Protection Officer; The Business Manager on behalf of the Board of Trustees

3. Procedure

Data Held and Processed

All staff, service users, volunteers and others are entitled to:

- Know what information the PROJECT CHALLENGE holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the PROJECT CHALLENGE is doing to comply with its obligations under the 1998 and 2000 Acts as well as GDPR

Personal Data:

- Must be fairly and lawfully processed
- Must only be obtained for specified and lawful purposes
- Must be adequate, relevant and not excessive in relation to the purpose for which it is required
- Must be accurate and, where necessary, kept up to date
- Must only be processed and kept for as long as is necessary
- Must be processed in accordance with the data subject's rights under the act
- Must be protected against unlawful processing, accidental loss and destruction or damage
- Must not be transferred to a country or territory outside the EEC, unless adequate levels of protection/freedoms are in place

Under GDPR, these eight principles are retained but summarised within a new six-point profile to which PROJECT CHALLENGE is committed: -

Accordingly, under GDPR, Personal Data we process should be:

1. Lawful, fair and transparent
2. Limited for its purpose
3. Adequate and necessary
4. Accurate
5. Kept only for as long as needed
6. Provide for Integrity and Confidentiality

Data Protection Controller

PROJECT CHALLENGE has registered under the Act with the Information Commissioner using the template provided for FE establishments. PROJECT CHALLENGE has a designated Data Protection Controller (The Business Manager), who is responsible for our registration under the Act.

General Data Protection Regulation (from 2018)

Initial preparation under the new regulation will include the following:

a) Awareness raising for key managers and staff within PROJECT CHALLENGE to understanding the impact of the legislation and compliance requirements
b) Documenting personal information that is held by PROJECT CHALLENGE including its source and where it is shared through an information audit, noting the legal basis for collection and processing
c) Making amendments to the information we give to staff and service users about how we will use their information (privacy notice) and how long it will be retained
d) Review PROJECT CHALLENGE processes for deleting personal data and electronic records including direct marketing implications
e) Review how PROJECT CHALLENGE responds to subject access requests within new reduced time limits
f) Review how consent is obtained and recorded with an effective audit trail, and including parental or guardian consent
g) Review procedures for detecting, reporting and investigating personal data breach
h) Implement a process to carry out Privacy Impact Assessments in high risk situations
i) Review the role of Data Protection Officer in the organisation

Project Challenge Protection Policy with GDPR

Requests for Information

a) Any service user, employee, client or person connected with PROJECT CHALLENGE may request details of information which they believe the organisation holds about them.

b) Any person seeking to request access to recorded information on us may do so by writing to the Freedom of Information Officer who is The Business Manager

PROJECT CHALLENGE will undertake to provide the requested information within 20 working days. The Freedom of Information Officer may refuse to disclose information where the disclosure is not in the public interest or where it could lead to a breach of the Data Protection Act.

Responsibilities of Staff

a) All staff, including those of other organisations delivering on behalf of the PROJECT CHALLENGE, are responsible for:

- checking that information provided to the organisation about their employment is accurate and up to date
- informing the organisation of any changes to information, i.e. change of address
- informing the organisation of any errors or changes. PROJECT CHALLENGE cannot be held responsible for any errors not reported to a member of staff

b) When, as part of their responsibilities, staff collect information about others (i.e. service users, students, volunteers, references, details of personal circumstances), they must comply with the procedure on personal data under 3 above.

c) The Data Protection Officer is responsible for keeping this policy updated and relevant

d) The Data Protection Officer must ensure that PROJECT CHALLENGE complies with the Data Protection Act 1998 and the new General Data Protection Regulation

Project Challenge Protection Policy with GDPR

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed in any way to any unauthorised third party. It should be noted that any unauthorised disclosure may be treated as a disciplinary matter and may be considered as gross misconduct

Personal information should be kept in a locked cabinet or locked drawer. Computerised information should be password protected and/or kept using a medium which is itself kept securely. Passwords should be changed on at least a quarterly basis.

Use of Portable Devices

a) Individuals who use a laptop, tablet or portable device to record, store, process or transmit PROJECT CHALLENGE-related data must do all that is reasonable to keep their device, associated media and the data contained therein secure always. Due to their portable nature, personal devices should not be left unattended when used off-site or during a journey, nor should they be left exposed on the seat of a car or other vehicle. Access should always be restricted by use of a system password.

b) When processing personal data on laptops or portable devices, all reasonable steps must be taken to ensure the security of that personal data. Personal data must not be processed in public places e.g. when travelling on public transport. All processing should be carried out in privacy to avoid accidental disclosure to non-authorised persons.

c) Individuals who use a small portable device to store PROJECT CHALLENGE-related data must do all that is reasonable to keep the device and the data contained therein secure always. Data must not be carried on small portable devices unless it is adequately secured. Access to the device should be protected by using a password or Personal Identification Number (PIN), if possible. Data encryption features should be utilised, where available.

d) Examples of small portable devices include:

- Palm-held and Pocket computers
- Tablets including PROJECT CHALLENGE issued i-pads
- Mobile Phones including smart phones
- USB Data Keys
- Removable Disk Drives
- Small memory cards (e.g. Sony Memory Sticks, Compact Flash memory, Smart Media cards, Multimedia cards, Secure Digital memory)

- Other storage media, including CD-ROMs, DVDs, floppy disks

e) Sensitive personal data, as defined in the Act, must not be stored in a portable device unless it can be demonstrated that special security precautions have been taken e.g. encryption of files on the hard disk or on a storage medium.

f) The Data Protection Officer should be contacted immediately in the event of the loss or theft of any portable device.

g) It should be noted that failure to implement appropriate security measures when using portable devices for the storage of personal data may be treated as a disciplinary matter and could be considered as gross misconduct.

References

Staff members who are requested to provide an employment reference in their professional capacity at PROJECT CHALLENGE should adhere to the following guidelines: -

- All data provided in a reference should be based on fact or should be capable of independent verification. As a guide, references should be fair, accurate and not give a misleading overall impression of the employee.
- Referees should avoid giving any subjective opinion about an individual's performance, conduct or suitability, unless it can be substantiated with factual evidence.
- The Referee has a duty of care to both the individual about whom it is written and the recipient of the reference, therefore references should be prepared with due care.
- The Business Manager should be contacted for further advice if there is any doubt or queries in relation to providing a reference.

Conclusion

Compliance with the Data Protection Act 1998 and the introduction of the General Data Protection Regulation is the responsibility of; The Board of Trustees, all members of PROJECT CHALLENGE and associated delivery staff. Staff should be mindful of the following:

- No undue pressure should be placed on anyone to disclose personal data
- No personal data should be disclosed over the telephone unless the caller has been properly identified and is entitled to the data
- Any special request for disclosure of personal data, e.g. to the Police or Inland Revenue, should be referred to the Data Protection Officer who will manage and log the request
- Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

4. Linked policies

- Freedom of Information Policy
- IT User Policy
- Information sharing

Appendix A – Glossary of Terms

1. Definitions

To make it easier to understand this policy, technical terms used are listed below:

Data Controller – Data Controller means a person who (either alone or with others) decides what personal information the agency will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person in an agency responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.

Data Subjects/Service Users – The individual whose personal information is being held or processed by an agency (for example: a client, an employee, a supporter).

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the data processing (see definition) of personal information (see definition) about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of an agency if an agency is a Data Controller (see above for definition). Certain activities may be exempt from notification.

2. Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998 and the GDPR

Processing **–** means collecting, amending, handling, storing or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about companies and agencies but applies to named persons or employees within an agency.

Project Challenge Protection Policy with GDPR

Sensitive data – means data about:

- ❖ Racial or ethnic origin
- ❖ Political opinions
- ❖ Religious or similar beliefs
- ❖ Trade union membership
- ❖ Physical or mental health
- ❖ Sexual life
- ❖ Criminal record
- ❖ Criminal proceedings relating to subject's offences

GDPR

The General Data Protection Regulation (GDPR) will apply from 25 May 2018.

It operates within a common set of rules applying across the (European Union) EU.

GDPR provides directions and information on: -

- Bigger Fines
- The Cloud
- Cookies
- Data Portability
- Privacy Impact Assessments
- Privacy Notices
- Reporting a Breach
- Profiling