

1. Data Protection & General Data Protection Regulation (GDPR) Policy

1.1 Purpose

The Data Protection Act & GDPR has two principal purposes:

1. To regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals, of those personal data.
2. To provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.

The Cornerstones of the Act are the eight data protection principles, which prescribe:

1. Guidelines on the information life-cycle (creation/acquisition; holding; processing; querying, amending, editing; disclosure or transfer to third parties and destruction ('the life-cycle')
2. The purpose for which data are gathered and held
3. Enshrine rights for data subjects

This policy has been written to acquaint staff with their duties under the Act & GDPR regulations and to set out the standards expected by BF Adventure in relation to processing of personal data and safeguarding individuals' rights and freedoms.

1.2 Staff duties

Employees of BF Adventure are expected to:

1. Acquaint themselves with, and abide by, the Data Protection Principles.
2. Read and understand this policy document, the BF Adventure Privacy Policy and Schedules 31 & 33 within the BFA Staff handbook.
3. Understand how to conform to the standard expected at any stage in the life-cycle (see section 4 of this policy).
4. Understand how to conform to the standard expected in relation to safeguarding data subjects' rights (e.g. the right to inspect personal data) under the Act.
5. Understand what is meant by 'sensitive personal data', and know how to handle such data.
6. Contact the Data Protection Officer if in any doubt, and not to jeopardise individuals' rights or risk a contravention of the Act.

1.3 The data protection principals

The data protection principles, in summary, are:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.
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.

1.4 Best-practice guidelines for the life-cycle process

1.4.1 Acquisition of personal data (see principles 1, 2, 3)

Those wishing to obtain personal data must comply with guidelines issued from time to time by the Data Protection Officer and, in particular, should tell data subjects the purpose(s) for which they are gathering the data, obtain their explicit consent, and inform them that BF Adventure will be the data controller for the purposes of the Act and the identities of any other persons to whom the data may be disclosed. If sensitive personal data are being collected, explicit consent is not only best practice, it is mandatory. No more data should be collected than is necessary for the purpose(s) declared.

1.4.2 Holding / safeguarding / disposal of personal data (see principles 4, 5, 7)

Data should not be held for longer than is necessary. Guidance for length of retention is set in law, or given in section 7.4.7 of this policy. Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken. This includes the protection of physical data through the use of locked storage, restricted access and a culture of respect for the information we hold, it also includes the protection of electronic data through restricting access to data and protecting data using passwords and encryption (further details of this can be found in the ICT policy).

1.4.3 Processing of personal data (see principles 1, 2)

In this particular context, 'processing' is used in the narrow sense of editing, amending or querying data. In the context of the Act as a whole, 'processing' is very widely defined to include acquisition, passive holding, disclosure and deletion.

Personal data must not be processed except for the purpose(s) for which they were obtained or for a similar, analogous purpose. If the new purpose is very different, the data subject's consent must be obtained.

1.4.4 Disclosures and transfers of personal data (see principles 1, 2, 7, 8)

1.4.5 Disclosures

BF Adventure's policy is to exercise its discretion under the Act to protect the confidentiality of those whose personal data it holds.

- i. Employees of BFA may not disclose any information about clients or other employees, including information as to whether or not any person is or has been a client or employee of the BFA unless they are clear that they have been given authority by BFA to do so. Particular care should be taken in relation to any posting of personal information on the internet.
- ii. No employee of BFA may provide references to prospective employers or landlords or others without the consent of the individual concerned. It is therefore essential that where BFA is given as a referee, the subject of the reference should provide BFA with the necessary notification and consent.
- iii. No employee may disclose personal data to the police or any other public authority unless that disclosure has been authorised by BFA's Data Protection Officer or Safeguarding Officers.
- iv. Employees of BFA may not use personal data for marketing (including photographs) without permission of the individuals, or the body/person with responsibility for those individuals (for example the school or parents of Clients).

1.4.6 Transfers

Personal data should not be transferred outside of BF Adventure and in particular, not to a country outside the EEA

- i. except with the data subject's consent; or
- ii. in accordance with a contractual data sharing agreement;
- iii. unless that country's data protection laws provide an adequate level of protection; or
- iv. adequate safeguards have been put in place in consultation with the Data Protection officer; or
- v. in consultation with the Data Protection Officer or Safeguarding Officer where it is established that there is a legal obligation to disclose, or that the Client may be at risk by non-disclosure (see the Confidentiality Policy).

1.4.7 Destruction of personal data (see principles 5, 7)

Personal data must not be held for longer than necessary; and when such data have been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

- Staff records – 25 years (in line with insurance guidelines for safeguarding young people)
- Client records – 5 years (unless otherwise directed by funders requirements)

1.5 Data subjects' right of access

BFA is fully committed to facilitating access by data subjects ('applicants') to their personal data, while bearing in mind the need to protect other individuals' rights of privacy.

All applicants will be expected to request access in writing or via email and will need to supply proof of identity before any data can be released. If a request is made by a third party BFA must be given adequate proof that the data subject has given authority to the third party for disclosure.

1.6 Review

This policy will be reviewed annually to take account of changes in the law and guidance issued by the Information Commissioner.

1.7 Data protection contacts

For general enquiries about the BF Adventure's Data Protection Policy and for formal subject access requests under the Act:

Data Protection Officer

BF Adventure

Goodygrane Activity Centre

Halvasso

Longdowns

Penryn

Cornwall

TR10 9BX

Tel: (01326) 340912 Email: enquiries@bfadventure.org

1.8 Disciplinary consequences of this policy

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA in contravention of paragraph 4.4.2 above) or any other breach of section 55 of the Data Protection Act & GDPR by staff, trustees or volunteers will be

treated seriously by BFA and may lead to disciplinary action up to and including dismissal or suspension.

Last update: Feb 2022

Updated by: Adrian Richards

To be reviewed by: March 2023