UK Society for Behaviour Analysis

DATA PROTECTION

POLICY

Committee responsible: Strategic Planning Committee
Approved by: UK-SBA Board
Date approved: January 2017

Date of last review: N/A
Date of next review: January 2018
Version number: 1

1. POLICY STATEMENT

UK-SBA refers to the UK Society for Behaviour Analysis.

This policy sets out UK-SBA's procedures for dealing with data protection and pays regard to the Information Commissioners Office (ICO) guidance. UK-SBA needs to collect and use certain types of information about the Individuals or Service Users who come into contact with UK-SBA in order to carry on our work. This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998. To do this, UK-SBA must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998.

We believe that all personal data covered by the Data Protection Act 1998 includes the members register, attendance registers, staff personnel files, financial information, strategic and improvement plans, records of contractors and suppliers.

UK-SBA will ensure that under the Data Protection Act 1998 all staff are able to access their personal data that is held about them. We believe it is our duty to respond to any request of access within 40 days. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

UK-SBA believes it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

2. AIMS

UK-SBA aims to fulfil our obligations under the Data Protection Act 1998 and to protect the right of staff and members to privacy in line with the Act.

- To allow all staff their right to have access to their personal data.
- To allow all members right of access to their records.
- To protect all staff to the right to privacy in line with the Data Protection Act 1998.
- To protect all members the right to privacy in line with the Data Protection Act 1998.
- To work with other organisations and external bodies to share good practice in order to improve this policy.

3. DATA CONTROLLER

UK-SBA is the Data Controller under the Act, which means that it determines what purposes personal information held or will be used for. UK-SBA 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 and ultimately is responsible for implementation. The designated data controller/s will deal with day to day matters.

All requests from staff for access to their data must be made in writing on headed note paper and sent to the data controller/s. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller/s initially. If the matter is not resolved it should be raised as a formal grievance.

4. RESPONSIBILITY FOR THE POLICY

The *Directors* have:

- the responsibility to comply with the legal requirements of the Data Protection Act 1998
- the responsibility to ensure data is processed in accordance with the eight principles of the Data Protection Act 1998
- delegated powers and responsibilities as the 'Data Controllers' for UK-SBA Trust
- delegated powers and responsibilities to ensure all staff and stakeholders are aware of and comply with this policy
- responsibility for ensuring that UK-SBA complies with all equalities legislation
- nominated a *committee* to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy

The Data Controller/s will:

- ensure security measures and confidential systems are in place to protect personal data and member records
- ensure data is obtained for specific and lawful purposes
- ensure data is adequate, relevant and not excessive
- ensure this policy and all policies are maintained and updated regularly
- ensure all policies are made available on request

All staff are responsible for:

- Checking that any information that they provide to UK-SBA in connection with their employment is accurate and up to date
- Informing UK-SBA of any changes to information, which they have provided, ie changes of address
- Informing UK-SBA of any errors or changes in staff information. UK-SBA cannot be held responsible for any such errors unless the staff member has informed UK-SBA of them.

Any personal data held will be kept securely, for example:

- Kept in a locked filing cabinet; or in a locked drawer;
- if it is computerised, be password protected; or
- kept only on disk, which is itself kept securely

5. DATA PROTECTION PRINCIPLES

Personal data means data which relate to an identifiable living individual and includes any expression of opinion about that individual. So personnel records, including sickness absence, performance appraisals, recruitment notes etc. will clearly be personal data. In addition, the DPA awards extra protection to certain types of personal data called sensitive personal data. This includes information about the subject's race, ethnicity, politics, religion, trade union status, health, sex life or criminal record. Such data will be treated with particular care. In addition, the ICO considers that financial data, although not technically defined as 'sensitive personal data' under the DPA should be treated in the same way. Together with information on race, religion or belief, union membership, sexual life and crimes, health information is classed as sensitive information by the law.

Processing information or data, means obtaining, recording or holding it or carrying out any operation on it, including its retrieval, consultation or use.

There are eight principles put in place by the DPA which specify that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than is necessary
- processed in line with an individual's rights
- secure
- not transferred to countries outside the EEA without adequate protection

6. DISCLOSURE OF DATA

Personal information will not be disclosed either orally or in writing to any unauthorised third party, without the consent of the individual except when it is legally required.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

7. REFERENCES

Unless a relevant exemption applies, data subjects have the right to request and be given a copy

of their reference. This depends, however, upon whether the request is made of the organisation providing the reference (usually the previous or current employer) or the organisation requesting the reference (the new or prospective employer). The recipient of a confidential reference can only disclose the reference by complying with the DPA's confidentiality rules. The referee who has given a confidential reference for employment, self-employment or educational purposes can withhold the reference from disclosure, though this only applies where the reference is given in confidence.

8. THE TELECOMMUNICATIONS (LAWFUL BUSINESS PRACTICE) REGULATIONS 2000

UK-SBA will also comply with the above regulations that were issued under Regulation of Investigatory Powers Act 2000 in order to comply with the EU's Telecommunications Data Protection Directive. They cover all types of telecommunications (telephone, email, fax, etc.) on public and private systems. UK-SBA may intercept these with the parties' consent.

UK-SBA can also intercept without consent:

- to establish facts
- to find out if a communication is for business or private purpose
- for quality control or training
- to comply with regulatory or self-regulatory procedures
- for system maintenance
- to detect unauthorised use
- to prevent or detect crime
- for national security purposes.

9. IMPLEMENTATION

The Board is responsible for ensuring that this policy is fully supported and complied with by all staff and that awareness of this policy will be raised via:

- UK-SBA's policies and procedures
- new staff induction, staff meetings and further communication channels within the organisation

The Board is responsible for ensuring that data

- shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

- shall be obtained only for one or more of the purposes specified in the act, and shall not be processed in any manner incompatible with that purpose or those purposes
- shall be adequate, relevant and not excessive in relation to those purpose(s)
- shall be accurate and, where necessary, kept up to date
- shall not be kept for longer than is necessary
- shall be processed in accordance with the rights of data subjects under the act
- shall be kept secure by the data controller/s who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information
- 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 individuals/service users in relation to the processing of personal information
- set out clear procedures for responding to requests for information

UK-SBA will, through appropriate management and strict application of criteria and controls:

- fully observe conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the rights of people about whom information is held, can be fully exercised under the act.

These include:

- the right to be informed that processing is being undertaken,
- the right of access to one's personal information
- the right to prevent processing in certain circumstances and
- the right to correct, rectify, block or erase information which is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

10. SUBJECT ACCESS REQUESTS

Directors, Staff, and Members within UK-SBA have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact the designated Data Controllers in the first instance.

There is a right to request in writing a copy in permanent form of the data held. UK-SBA will make a charge on each occasion that access is requested.

UK-SBA aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days from payment of the fee and evidence to confirm the identity.

11. MONITORING AND REVIEW

The practical application of this policy will be reviewed bi-annually or when the need arises by the *Board*. UK-SBA will regularly review and audit the ways it hold, manage and use personal information. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

APPENDICES

Related Documents

Document/Reference	Copy Location
ICO Subject Access Code of Practice	https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf
CIPD Data Protection Guide	http://www.cipd.co.uk/hr-resources/factsheets/data-protection.aspx
Information rights	https://ico.org.uk/media/for-organisations/documents/1568/information_rights_top_tips.pdf