



# Data Protection Policy

---

In compliance with the principals of the Data Protection Act 1998

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Contents

Introduction .....	3
Status of the Policy .....	3
The Data Controller and the Designated Data Controller.....	4
Responsibilities of Staff.....	4
Staff Information.....	4
Data Security.....	4
Responsibilities of Practitioners.....	4
Right to Access Information.....	5
Subject Consent and Processing Sensitive Information.....	5
Personal Data.....	5
Sensitive Data.....	5
Retention of Data.....	6
Conclusion.....	6
Data Protection Act 1998.....	7
Guidelines for Members of Staff.....	7
Staff Checklist for Recording Data .....	7
Glossary of Terms.....	7
Data.....	7
Personal Data .....	8
Sensitive Data.....	8
Data Subject .....	8
Data Controller.....	9
Data Processor .....	9
Processing .....	9
Consent .....	9
Recipient .....	9
Third Party.....	9

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Introduction

DSA-QAG ("the organisation") retains certain information about its employees, practitioners and other users to allow it to monitor performance, achievements, and health and safety, for example. It also needs to process information so that members of staff can be recruited and paid, support for practitioners organised (e.g. assessment centres, outreach centres, assistive technology service providers and non-medical helper organisations) and obligations to stakeholders and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Organisation must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998.

In summary these state that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and kept up-to-date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the Data Subject's rights.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The Organisation and all members of staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Organisation has developed this Data Protection Policy.

## Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the Organisation from time-to-time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any practitioner or 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 initially. If the matter is not resolved it should be raised as a formal grievance.

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## The Data Controller and the Designated Data Controller

The organisation is the Data Controller under the Act, and the Trustees are therefore ultimately responsible for the implementation of the Data Protection Policy. However, the Designated Data Controller will deal with day-to-day matters.

The Organisation has appointed the Operations Manager to act as Designated Data Controller and Data Protection Officer. Any query relating to the implementation of the Data Protection Act 1998 should be referred to the Designated Data Controller (administration@dsa-qag.org.uk).

## Responsibilities of Staff

### Staff Information

All members of staff are responsible for:

- Checking that any information they provide to the organisation in connection with their employment is accurate and up-to-date.
- Informing the organisation of any error or change to the information they have provided, for instance a change of address. The organisation cannot be held responsible for any such errors unless the member of staff has informed the organisation of them.

### Data Security

When, as part of their responsibilities, members of staff collect information about other people, (for instance about practitioners), they must comply with the Guidelines for Members of Staff (Appendix 1).

All members of staff are responsible for ensuring that:

- Any personal data held by them is kept securely, for instance, computerised data, should be password protected; and
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

Members of staff should note that unauthorised disclosure will usually be a disciplinary matter, and may also result in a personal liability for the individual member of staff.

## Responsibilities of Practitioners

Practitioners should ensure that all personal data provided to the Organisation (such as telephone numbers, addresses or email addresses) is accurate and up-to-date.

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Right to Access Information

As per the Data Protection Act 1998, members of staff, practitioners and other Data Subjects of the organisation have the right to request access to 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 complete a Subject Access Request in writing and submit it to the Designated Data Controller (see above).

In all cases where data is requested, the organisation will charge £20 on each occasion that access is requested.

The organisation aims to comply with requests for access to personal information as quickly as possible, but will ensure it is provided within 40 days.

## Subject Consent and Processing Sensitive Information

### Personal Data

The organisation has to process personal information to efficiently manage its day-to-day operations and operate other policies, such as its equal opportunities policy

Agreement to the organisation processing some specified types of personal data is a condition of becoming a DSA-QAG practitioner, and a condition of employment for members of staff.

Some examples of the ways in which this data may be used are set out below:

- Informing a university about their background information or progress.
- Informing a practitioner on the progress of their application
- Sharing an Employee's address with our payroll company.

A list of what information we consider to be personal data can be found in the Glossary section.

### Sensitive Data

The organisation may also have to process some sensitive personal information to best serve its charitable purpose. Agreement to the organisation processing some specified types of sensitive data is a condition of becoming a DSA-QAG practitioner, and a condition of employment for members of staff. This includes past criminal convictions.

However, we will not share your sensitive information with a third party without obtaining your explicit consent.

In compliance with the Data Protection Act 1998, a list of types of information that are considered to be sensitive data can be found in the Glossary section.

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Retention of Data

Different categories of data will be retained for different periods of time. The organisation will need to keep some data on members of staff and practitioners indefinitely. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, information required for job references as well as for future research.

Any sensitive information held on a DSA-QAG practitioner will either be disposed of, or if needed for future research, anonymised one year after the practitioner has ceased their relationship with the Organisation.

In the case of individuals who apply to become practitioners but are rejected, the organisation will delete all information other than: name, email address, and reason for rejection, one year after their application was made. This remaining information will be kept indefinitely.

## Conclusion

Compliance with the Data Protection Act 1998 is the responsibility of all members of the organisation. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to organisation facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Designated Data Controller.

The organisation is obliged to abide by all legal requests for information made by law enforcement or judicial bodies.

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Data Protection Act 1998

### Guidelines for Members of Staff

1. Members of staff will process personal and sensitive data on a regular basis. The Organisation will ensure that members of staff and practitioners give their consent to processing and are notified of the categories of processing, as required by the Act.
2. Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the organisation's Data Protection Policy. In particular, members of staff must ensure that records are:
  - accurate;
  - up-to-date;
  - kept and disposed of safely, and in accordance with the organisation policy.
3. Individual members of staff are responsible for ensuring that all data they are holding is kept securely.
4. Individual members of staff are responsible for ensuring that paper records are destroyed securely, preferably shredded.
5. Guidance can be obtained from the Operations Manager regarding the safe disposal of electronically stored data.
6. Members of staff should also refer to and comply with the organisation's additional internal guidance on the use of personal electronic devices for work purposes.
7. Before processing any personal or sensitive data, all members of staff should consider the checklist.

### Staff Checklist for Recording Data

1. Do you really need to record the information?
2. Is the information 'personal' or is it 'sensitive'?
3. If it is sensitive and is being transferred to a third party, do you have the Data Subject's express consent?
4. Has the individual or Data Subject been told that this type of data will be processed?
5. Are you authorised to collect/store/process the data?
6. If yes, have you checked with the Data Subject that the data is accurate?
7. Are you sure that the data is secure?
8. If you do not have the Data Subject's consent to process, are you satisfied that it is in the best interests of the practitioner or the member of staff to collect and retain the data?
9. How long do you need to keep the data for, and what is the mechanism for review/ destruction?

## Glossary of Terms

### Data

Any information which will be processed, or, used on or by a computerised system, additionally it also includes information contained within a "relevant filing system" of information. Data can therefore be written, tape, photographic or digital.

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Personal Data

Personal data means data which relates to a living individual who can be identified:

1. from that data; or
2. for that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller; and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Examples of data which would fall into this category include:

- Names
- Gender
- Date of birth
- University details
- Emails, phone number and personal address
- IP address from where registration forms are sent
- Postcode
- References
- Qualifications
- Career interests
- Interview question answers
- Applications

## Sensitive Data

This means data which relates to sensitive aspects of a living and identifiable individual's life

Examples of data which would fall into this category include:

1. Family income
2. Number of active guardians
3. Parents' occupation, employment etc.
4. Student Finance arrangements
5. Information relating to siblings
6. Mitigating circumstances
7. Photos of an individual
8. Photos of student finance documents
9. Disability information
10. Equal opportunity information - ethnicity, sexual orientation, religion, marital status etc.
11. Free School Meal eligibility
12. Whether or not a person is a care leaver
13. ACORN deprivation data

## Data Subject

The person who is the subject of the "personal data".

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------

## Data Controller

A person who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

## Data Processor

Any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller. The Data Controller retains responsibility for the actions of the Data Processor.

## Processing

Covers almost anything which is done with or to the data, including:

- obtaining data;
- recording or entering data onto the files;
- holding data, or keeping it on file without doing anything to it or with it;
- organising, altering or adapting data in any way;
- retrieving, consulting or otherwise using the data;
- disclosing data either by giving it out, by sending it on email, or simply by making it available;
- combining data with other information;
- erasing or destroying data; and
- using the data within research

## Consent

The European Data Protection Directive defines this as “any freely given specific and informed indication of his wishes by which the Data Subject signifies his agreement to personal data relating to him being processed”. Consent can be withdrawn after it has been given.

Where data is “sensitive”, express consent should be sought before the data is given to a third party.

## Recipient

Under the Data Protection Act a recipient is defined as “any person to whom the data are disclosed, including any person to whom they are disclosed in the course of processing the data for the Data Controller (e.g. an employee of the Data Controller, a Data Processor or employee of the Data Processor)”.

## Third Party

The Data Protection Act defines a “third party”, in relation to personal data, as “any person other than -

- the Data Controller, or
- other persons authorised to process data by the Data Controller.”

“Third party” does not include employees or agents of the Data Controller or Data Processor of staff members.

Owner: <b>DSA-QAG</b>	Date: <b>01/12/2015</b>	Version: <b>1.0</b>	Status: <b>Final</b>	data protection policy v1.0 011215
--------------------------	----------------------------	------------------------	-------------------------	------------------------------------