



## DATA PROTECTION POLICY

### 1. Introduction

The Data Protection Act 1998 imposes controls on the type of information that public bodies can collect, hold or disclose about current, potential or former recipients of services. It also sets out conditions, which must be satisfied before certain types of information can be held or otherwise processed.

In order to fulfil its aims and objectives, good practice and legal obligations, NASMA as a membership organisation, collects, holds and processes information about its members. In addition to members information NASMA will also collect, retain and process data for those attending training or other events.

In respect of members and training delegates, NASMA will collect, hold and process personal data, including 'sensitive personal data'.

Those whose data is retained will be made aware that records are being kept, given an explanation of the purpose they are kept for and the nature of any intended disclosures, unless the details are self evident.

The personal data that NASMA will collect and keep for current, past or prospective members will be in relation to matters in direct relationship to the services that are being accessed, and also any information collated as part of monitoring or assessment procedures.

All staff who process or use any personal information, in order to execute these obligations, will comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

### 2. The Data Protection Principles

The Act lays down 8 principles governing the processing of personal data. In summary, these state that personal data shall:

- Be processed fairly and lawfully
- Be obtained for a specific and lawful purpose
- Be adequate, relevant, and not excessive for those purposes
- Be accurate and up to date
- Not be retained for longer than is necessary for the purpose for which it was obtained
- Be processed in accordance with the rights of the data subject
- Be kept safe from unauthorised processing, and accidental loss, damage or destruction
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.



Delivering an effective  
support network since 1995



## National Association of Student Money Advisers

### 3. Definitions

The Act defines the following:

- 3.1 **'Personal data'** is information about a living individual, either processed by a computer or where manual, which forms or is intended to form part of a relevant filing system.
- 3.2 **'Sensitive personal data'** is information about a person's racial or ethnic origins, political opinions, religious beliefs, trade union membership, health, sexual life or any criminal offences. This information is subject to more stringent controls.
- 3.3 **'Relevant filing system'** is one in which the data is structured in such a way that specific information relating to a particular person is readily accessible.
- 3.4 **'Processing'** covers everything you might do with data such as obtaining, recording, storing, disclosing, copying adding, deleting, extracting and destroying information.
- 3.5 **'Data subject'** refers to a living individual who is the subject of personal data. The individual may be a current, past or prospective NASMA member.
- 3.6 **'Data controller'** NASMA, as a corporate body is the 'data controller' under the Act and the Board of directors is therefore responsible for implementation.

### 4. Access to Personal Data

- 4.1 All personal data, including 'sensitive personal data' must be kept secure. Access will only be granted to those relevant individuals who may require access for the proper performance of their duties and for a specific purpose. For the purposes of NASMA this would normally be NASMA directors & employees.
- 4.2 Where information is collected, all individuals will have the right to know the purpose for which the personal data is used and the right of access to any personal data that is being kept in a 'relevant filing system' (both electronically and paper based). They also have the right to the identity of all other keepers of personal data.
- 4.3 Individuals may exercise their right to view their personal records by giving at least 5 working days notice to the "data keeper" who shall be the relevant staff member, or their designate.
- 4.4 When an individual requests access to view their personal file NASMA will arrange an appointment with the individual to come to view the file, or arrange for a copy of the file to be posted. Individuals attending to



Delivering an effective  
support network since 1995



## National Association of Student Money Advisers

view their file may also request a full photocopy. A member of staff will be available during the viewing of the file to give assistance such as making photocopies of particular items that may be required. However the removal of documents from files will be strictly forbidden.

4.5 Individuals are entitled to make a reasonable request for the amendment of their personal data provided that they can readily demonstrate the existence of an identifiable error or that it is unlawful to process such data.

4.6 The following data is exempt from subject access:

- Personal data relating to another party, or data through which personal data about another party could be discerned.
- Individuals will not be given their personal data where the release of information would be likely to prejudice the conduct of business.

### **5. Retention of Data**

NASMA will only retain personal information that is necessary and legal to keep.

### **6. Disposal of Records**

NASMA is obliged under the Act to dispose of personal information when it is no longer needed or necessary. To prevent unauthorised or accidental disclosure of information, keepers of such information will exercise care in its disposal, including assuring its protection, security and confidentiality during storage, transportation, handling and destruction. Paper records containing personal information will be shredded. Care will also be taken with electronic records, which can be reconstructed from deleted information.

### **7. Security**

In order to eliminate unauthorised access and minimise risk of accidental loss, destruction or damage, Personal records will be kept in secure filing systems under lock and key. Personal data held on computerised systems will be password protected for authorised access only.

### **8. Compliance**

Compliance with the Act is the responsibility of all the individuals involved in a process. Failure to comply with the policy may result in disciplinary action. Any member of staff who considers the policy has not been followed in respect of personal data about clients, should raise the matter with the NASMA Board of directors.