| Reference | H&A – POL 00 |
|---|---|
| Version | 1.0 |
| Issue Date | 01/10/2016 |
| Approved | MD |

# H&A Protection Services

# Data Protection Policy

## 1. PURPOSE

This policy applies to H&A Protection services in England. The company Is registered with the Information Commissioner and complete details of the current entry on the Data Protection Register can be found on the notification section of the Information Commissioners web site. www.dataprotection.gov.uk.

The register entry provides:

• a fuller explanation of the purposes for which personal information may be used
• details of the types of data subjects about whom personal information may be held
• details of the types of personal information that may be processed
• details of the individuals and organisations that may be recipients of personal information collected by H&A Protection Services
• information about transfers of personal information the company Needs to keep certain information about its employees, students, voluntary members and other users for academic and administrative purposes. It also needs to process information so that legal obligations to funding bodies and government are complied with. When processing such information, the company Must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998. Anyone processing personal data must comply with the eight enforceable principles of good practice. In summary these state that personal data shall be:
• fairly and lawfully processed;
• processed for limited purposes;
• adequate, relevant and not excessive;
• accurate;
• not kept longer than necessary;
• processed in accordance with the data subject's rights;
• secure;
• not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. With processing, the definition surrounding the intentions of the **data controller** towards the individual, are far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'. H&A Protection Services Staff or others who process or use personal information must ensure that they follow these principles at all times.

## 2. RESPONSIBILITY

The Director is responsible for ensuring that this policy is applied within the association.

The Management Rep is responsible for maintenance, regular review and the updating of this policy.

## 3. STATUS OF THE POLICY

This document sets out the H&A Protection Services policy and procedures to meet the requirements of the Data Protection Act 1998. It will be made available to employees, students, and voluntary members and other external agencies (having a legitimate interest) upon request, although it is not a substitute for the full wording of the Act.

## 4. THE DATA CONTROLLER

The Management Rep is ultimately responsible for Data Protection, but the Director of Resources is regarded as the main Data Controller. In practice local Regional staff are designated as local data protection officers to deal with day to day matters and ensure they comply with the Data Protection Act on an ongoing basis. They will often look to Course Managers for support in this.

## 5. SUBJECT CONSENT

In many cases, H&A Protection Services can only process personal data with the consent of the individual and if the data is sensitive, express consent must be obtained. Agreement to the company Processing some specified categories of personal data is a condition of acceptance of a student onto any course, membership of the Association being recognised, and a condition of employment for staff. For example, this includes information about previous criminal convictions, in accordance with the Rehabilitation of Offenders Act 1974. Some jobs or courses or other company Activities, will bring staff, students and voluntary members into contact with children, including young people between the ages of 16 and 18 or vulnerable adults. The company has a duty to ensure that all staff are suitable for the job, students for the courses offered, and
voluntary members for the company Activity are involved. We also have a duty of care to all staff, students and voluntary members and must therefore
make sure that employees and those who use H&A Protection Services Facilities do not pose a threat or danger to other users. Therefore, all prospective staff, students and voluntary members will be asked to consent to their data being processed when an offer of employment, course place or inclusion in other company Activities. A refusal to give such consent may result in the offer being withdrawn. Other relevant policies here are the Criminal Disclosure Checks and Child Protection Policies.

## 6. STAFF RESPONSIBILITIES (INCLUDING SECURITY PERSONS)

This policy will not be incorporated into contracts of employment, but it is a condition of employment that employees will abide by the rules and policies made by H&A Protection Services From time to time. Any failures to follow this policy can therefore result in disciplinary proceedings. 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 Data Controller. If raising the issue with the Data Controller does not resolve it the matter should be raised as a formal grievance.

### 6.1. **Specific Staff Responsibilities**

All staff, including temp and staff such as security persons, have a responsibility for:

• Checking that any information that they provide to the company in connection with their employment is accurate and up to date.

• Informing H&A Protection Services Of any changes to information, which they have provided, i.e. changes of address, bank details, etc.

• Informing the company Of any errors or changes in staff information. When staff hold or process information about students, colleagues or other data subjects (for example, students' course work, references to other academic institutions, or details of personal circumstances), they should comply with the following Data Protection Guidelines:

All staff are responsible for ensuring that:

• Any personal data, which they hold, is kept securely, for example:
o kept in a locked filing cabinet; or
o in a locked drawer;
o if it is computerised, be password protected; or
o kept only on disk, which is itself kept securely.

• Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Any unauthorised disclosure will be investigated as 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, as unauthorised disclosure can be a criminal offence.

6.2. **Staff Use of Personal Data Off-Site, On Home Computers or at Remote Sites**

Employees processing personal data off-site should ensure they take reasonable precautions to prevent the data from being accessed, disclosed or destroyed as a result of any act or omission on their part. They should notify the Data Controller immediately in the event of any loss or theft.

## 7. VOLUNTARY MEMBERS OBLIGATIONS

Voluntary Members should ensure that all personal data provided to H&A Protection Services is accurate and up to date. They should also ensure that changes of address, etc are notified to the Office Manager as appropriate.

Any member of the company, who considers that the policy has not been followed in respect of personal data about him or herself, should raise the matter with the Office Manager initially. If the matter is not resolved informally it should then be raised with the Data Controller, and if it is still not resolved it should be raised as a formal complaint through the voluntary member complaint procedure.

7.1. **Responsibilities of Voluntary Members**

All voluntary members who are active in the organisation and who may have access to, hold or store personal data on other members, staff or students, should comply with this policy and follow the company Data Protection Guidelines for third party associates:

All voluntary members are responsible for ensuring that:

• Any personal data, which they hold, is kept securely, for example:
o kept in a locked filing cabinet; or
o in a locked drawer;
o if it is computerised, be password protected; or
o kept only on disk, which is itself kept securely.

• Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Voluntary Members should note that unauthorised disclosure may result in a personal liability for the individual voluntary member, as unauthorised disclosure can be a criminal offence. Any unauthorised disclosure will be investigated as a disciplinary matter and dealt with under the process contained in the company Volunteer Policy.

## 7. STUDENT OBLIGATIONS

Students must ensure that all personal data provided to the company Is accurate and up to date. They must ensure that changes of address, etc are notified to Regional office staff as appropriate.

### 7.1. **Student Personal Information – The Purposes for Which it is Used**

Information that we collect, including information that students give us at registration, is added to a record. H&A Protection Services Holds general information about students, such as name, address, courses studied and fee payments, and data to do with individual learning plans, examinations, assessments, course results and other achievements. (Some data relevant to exams and assessment are destroyed shortly after the course result is decided, and only the result itself is kept.) Personal information is used in the following ways:

• To process applications.
• To provide services to applicants and students. This includes sending information about current and future study opportunities with the company.
• To undertake research in order to help us plan and improve our services. We may contact applicants or students ourselves.
• To provide information about students to other bodies in accordance with government requirements e.g. to the local authorities, the Scottish Executive and other funding or governmental bodies.
• To provide information about students to other bodies in order to provide accreditation and for audit purposes.
• To enable other organisations to provide services to students e.g. other institutions who provide educational services as part of our programmes.
• To produce statistical information for publication and to help us plan and improve our services.

Student personal data record will show whether or not the individual consented to be contacted for audit purposes. Student records may be added to a database which may be passed to government departments and agencies and devolved administrations which require it to enable them to carry out their functions under the Education Acts. It will also be used in anonymous form for statistical analysis.
Contact details will not be made available, unless individuals have indicated their consent to be contacted as part of an audit of H&A Protection services. Names will not be used or included in its statistical analysis and precautions are taken to minimise the risk that individuals will be able to be identified from the data.

8.2. **Examination Marks / Accreditation**

Students will be entitled to information about their marks for both coursework and examinations as part of their support. This is within the provisions of the Act relating to the release of data. However, this may take longer than other information to provide.

**9. ACCURACY OF DATA**

Updating is required only "where necessary" on the basis that, provided the company Has taken reasonable steps to ensure accuracy (e.g. taking up references), data held is presumed accurate at the time it was collated. All employees, students and voluntary members should be made aware of the importance of providing the company with notice of any change in personal circumstances.

Where Individual Student Records (ISRs) are kept, students will be made aware of who to contact in order to access the data for the purposes of ensuring that the data is up to date and accurate. Employees, students and voluntary members will be entitled to correct any details although in some cases the company may require documentary evidence before effecting the correction, e.g. by seeking examination or qualification certificates for amending qualification details.

**10. THIRD PARTIES**

Any personal data which the company Receives and processes in relation to third parties, such as visitors, suppliers, former students and voluntary members, employers, enquirers and other individuals on mailing lists etc. will be
obtained lawfully and fairly and dealt with in accordance with the principles and conditions of the Act. Employees should obtain explicit consent from third party data subjects to process such personal data for the purposes expressed and should ensure that there is a mechanism for data subjects to gain access to data about themselves, to prevent the processing of such data for the purposes of direct marketing and to object to the disclosure of such data.

**11. SECURITY MEASURES**

This policy is designed to fulfil security person requirements and to prevent unauthorised disclosure of/or access to personal data. The following security measures will therefore be required in respect of the processing of any personal data. Access to personal data on staff, students and voluntary members is restricted to those members of staff who have a legitimate need to access such data in accordance with the company notification to the Information Commissioner.
Members of staff authorised to access personal data, will be allowed to do so, only in so far as they have a legitimate need and only for the purposes recorded in the notification. All persons processing data and individuals requesting access to personal data in accordance with this policy must have familiarised themselves with

this policy. All personal data will be stored in such a way that access is only permitted by authorised staff, including storage in filing cabinets, computers and other storage systems. Any act or omission which leads to unauthorised access or disclosure could lead to disciplinary action. Personal data should be transferred under conditions of security commensurate with the anticipated risks and appropriate to the type of data held. Personal data held electronically should be appropriately backed up and stored securely to avoid incurring liability to individuals who may suffer damage or distress as a result of the loss or destruction of their personal data.

Any disposal of personal data will be conducted in a secure way, normally by shredding. All computer equipment or media to be sold or scrapped must have had all personal data completely destroyed, by re-formatting, overwriting or degaussing (a method of erasing data held on magnetic media).

### 11.1. Retention of Data

The company Will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements.

### 11.2. Transfer of Data Outside the UK

H&A Protection Services Does not transfer personal data outside the UK without the express consent of the data subject.

## 12. USE OF PERSONAL DATA IN RESEARCH

The 1998 act provides certain exemptions for 'research purposes' including statistical or historical purposes. Provided that the purpose of research processing is not measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, then personal data may be: