Data Protection Policy & Code of Practise

Contents

1 Data Protection Policy

Introduction

1. appa training needs to keep certain information about employees, students and others users to allow it to monitor performance, achievements and health and safety, for example. It is also necessary to process information so that the centre can comply with its legal obligations and staff can be recruited and paid and courses organised. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2. To do this appa training must comply with the seven key principles of the General Data Protection Regulation (GDPR).

3. In summary these state that personal data shall:

a) Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
b) Be obtained for a specific and lawful purpose and shall not be processed in any manner incompatible with that purpose
c) Be minimal in nature. Data must be adequate, relevant and limited to the specific purposes of appaTraining.
d) Data must be accurate and kept accurate.
e) Be kept in a form that allows subject identification for no longer than necessary.
f) Be kept safe from unauthorised access, accidental loss or destruction
g) Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

4. appa training and all staff or others who process of use personal information must ensure that they follow these principles at all times

5. In order to ensure that this happens, the centre has developed this Data Protection Code of Practice and the accompanying Data Protection Code of Practice.

6. Status of this policy

This policy does not form part of the formal contract of employment for staff, or the formal offer of a place for study for students, but it is a condition of employment tor study that employees and students will abide by the rules and policies made by the centre from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings

7. The Data Controller and the Designated Data Controllers.

The centre as a body corporate is the Data Controller under the 1998 Act, and the Directors are therefore ultimately responsible for the implementation. However, the Designated Data Controllers will deal with day-to-day matters.

8. The centre has 2 Designated Data Controllers. They are the Facilities Manager and the Memberships Coordinator.

9. Any member of staff, student, applicant or other individual who considers that the Policy has not been followed in respect of personal data about their self should raise the matter with the appropriate Designated Data Controller, who would be:

For students: Facilities Manager
Staff/All Others: Memberships Coordinator

10. The administrative departments will themselves have designated staff who will provide details of the data held in their departments.

11. Responsibilities of Staff

All staff are responsible for:

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

- Informing the centre of any changes to information that they have provide, e.g change of address, either at the time of appointment of subsequently. The centre cannot be held responsible for any errors unless the staff member has information the centre of such changes.

12. If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other educational institutes, or details of personal circumstances), they must comply with the guidelines for staff set out in paragraphs 10-13 of the centres Data Protection Code of Practice.

13. Student obligations

Students must ensure that all personal data provided to the centre is accurate and up to date. They must ensure that t changes of address etc. are notified to student support.

14. Students who may from time to time process personal data as part of their studies must notify their supervisor/tutor, who should inform the student support

team, and must comply with the guidelines for data collection and security as set out in paragraphs 10-26 of the centres Data Protection Code of Practise

15. Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

16. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

17. Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe:
  or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up;
  and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

18. Further information on data security is given in paragraphs 14-36 of the centres Data Protection Code of Practise

19. Rights to access information

All staff, students and other users are entitled to:

- Know what information the centre holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the centre is doing to comply with its obligations under the GDPR

20. This policy document and the centres Data Protection Code of Practice address in particular the last three points above. To address the first point, the centre will, upon request, provide all staff and learners and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the centre holds and processes about them, and the reasons for which they processed.

21. All staff, learners and other users have a right under the GDPR to access certain personal data being kept about them either on computer or in certain fields. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the appropriate Designated Data Controller (See above).

22. The centre will make a charge of £15 on each occasion that access is requested, although the centre has discretion to waive this.

23. The centre aims to comply with requests for access to personal information as quickly as possible, as required by the GDPR, but will ensure that it is provided within 40 days

24. Examination Marks

During the course of their studies, learners will routinely be provided with information about their marks for both coursework and examinations. However, exam scripts themselves are exempted from the subject access request and copies will not ordinarily be given to a learner who makes a subject access request. Further details are given in paragraph 38 of the centres Data Protection Code of Practise

25. Subject consent

In many cases, the centre can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the centre processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

26. Some jobs or course will bring the applicants into contact with children, including young people between the ages of 16 and 18. The centre has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students for the course offered. The centre also has a duty of care to all staff and learners and must therefore make sure that employees and those who use centre facilities do not pose a threat or danger to other users.

27. The centre may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The centre will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

28. Therefore, the application forms that all prospective staff and students are required to compete will include a section requiring consent to process the applicant's personal data. A refusal to sign such a

form will prevent the application from being processed.

29. Processing sensitive information

Sometimes it is necessary to process information about a person's health, criminal convictions, race, and trade union membership. This may be to ensure that the centre is a safe place for everyone, or to operation other centre policies, such as the sick pay policy or the equal opportunities policy. Because this information is considered sensitive under the GDPR, staff (and students where appropriate) will be asked to give their express consent for the centre to process this data. An offer of employment or a course place may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from the Designated Data Controllers.

30. Publication of college information

The names of senior officers and governors of the college or any other personal data relating to employees of governors will be published in the annual calendar and on the public web site when any statute or law requires such data to be made public.

31. Certain items of information relating to centre staff will be made available via searchable directories on the public web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with appropriate staff. Paragraph 27-30 of the centres Data Protections Code of Practice set out the details of this scheme.

32. It may be the case that students enrolled on certain courses may produce web-based material containing personal data as part of their course work. All such activities are set out in detail in paragraphs 27-31 of the Centres Data Protection Code of Practice.

33. Retention of Data

The centre has a duty to retain some staff and student personal data for a period of times following their departure from the centre, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time, the exact details of retention periods and purposes are set out on pages 11-12 of the centres Data Protection Code of Practice.

34. Conclusion

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

2 Data Protection Code of Practice

1. Introduction

This code of practise must be read in conjunction with the centres Data Protection Policy document to give the fullest picture of appa trainings data protection regime. This document gives an introduction to some basic points of practice relating to the handling and processing of personal data at appa training. It also lists the particular activities carried out within the centres administrative and academic departments that involves the handling and processing of personal data.

2. Key concepts

The GDPR places an obligation upon appa training, as a data controller, to collect and use personal data in a responsible and accountable fashion. Appa training is committed to ensuring that every current employee and registered students complies with this Act to ensure the confidentiality of any personal data held by the centre in whatever medium. Three key concepts to be considered are those of purpose, fairness and transparency.

3. Purpose

Data controllers can only process personal data where they have a clear purpose for doing so and then only as necessitated by that purpose. Paragraphs 39-50 of this Code of Practice summarise the purposes for which the centre processes personal data. Personal data cannot be processed for purposes that have not been defined and declared in the centres Data Protection Register entry (see paragraph 6 below).

4. Fairness

In defining the purposes for which appa training processes personal data, the fairness of the processing must be considered for some types of processing the required elements of fairness are legality are clearly outlined in the legislation, but for many others they are not, in such cases, appa has tried to take a broad approach to deciding what is fair in each case, based on an interpretation of the 1998 Act and in conjunction with advice from the Information Commissioner, the centres own legal advisors, and on wider practice within the UK HE sector.

5. Transparency

Members of staff, students and others must be able to feel that there is no intention to hide from them details of how their personal data are connected, used and distributed by the centre. One of the functions of this Code of Practice is to provide that assurance.

6. Existing Notifications

The Act requires many data controllers to notify the Information Commissioner for the purposes for which personal data are processed, together with certain details of that processing, those notifications are then held on a private database.

7. It is an offence for the centre to hold personal data that falls outside of the classes declare n these notifications or to process personal date for any purposes that are not defined there. It is therefore very important that those who work with personal data in the course of their centre duties are familiar with the details contained in these notifications.

8. Any changes that may be required should be passed to the centre student support officers as these entries are periodically reviewed and amended as necessary by the centre.

9. Paragraph 35 of this Code of Practice gives details of the centre Designated Data Controllers, who are responsible for handling subject access requests and dealing with data protection enquiries within the centre.

Collection and Amendment of Personal Data

10. Collection of personal data

In most cases, the personal data held by the centre will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data. Amy members of staff responsible for managing the collection of personal data for the legitimate activities of the centre must ensure that a notice containing the following information is included in the request for that data.

- A statement that appa training is the data controller.
- The name and or job title of the specific member of staff responsible for the administration of the personal data being collected, to, enable, for example, subsequent amendments to be submitted by the data subject.
- A clear explanation of the types of data being collected and the purposes for which that data will be processed.
- Any further information that is considered necessary to ensure that the data processing can be described as being fair, for example details of any third parties to whom the data might be disclosed.
- A statement making it clear that by submitting the personal data, the data subjects are giving their consent of the processing of the data for the stated purpose to take place.

11. Amendment of personal data

From time to time data subjects will wish to update some of their personal data held by the centre, for example their home addresses of other contact details previously submitted. To do this, the data subjects must either contact the specific member of staff designated in the data protection notice at the time the data was submitted, or the appropriate Designated Data Controller as set out in paragraph 35. Proof of identity will be required before any amendments can be made.

12. As and when 'self-service' computer-based administrative systems are introduced for staff, students or others, the data subjects themselves will be able to take responsibility for the maintenance of certain elements of their personal records.

13. These systems will incorporate the necessary authentication and security mechanisms to ensure that data subjects are only able to view and amend their own data.

14. Security of personal data

Of fundament importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside the centre. Authorised disclosures or transfers are those that are defined within the appropriate notifications (see paragraphs 6-9 above) and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required.

15. To help ensure the security of personal data within the centre, all those working in the centre who process such data in the course of performing their duties are required to follow the general guidelines set out below.

16. Secure storage of personal data

Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with appa training Data Protection Policy, which states that personal data should:

- Be kept in a locked filing cabinet, drawer, or safe:
  Or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up:
  And
- If a copy is kept on a diskette or other removable storage media, that media, must itself be kept in a locked filing cabinet, drawer, or safe

17. Ordinarily, personal data should never be stored at staff members 'homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

18. Staff should be aware that log files would record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data

19. **Secure processing of personal data**
While staff members in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and pricey of that data. For example:
    - Open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff may readily see that data, and password-protected screensavers should be used
    - Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or at least covered,
    - Where manual records containing personal data are accessible to a number of staff in the course of their legitimate activities, access logbooks should be used where practicable to help monitor the whereabouts and use of the such records

20. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the centre manager must be obtained, and all the security guidelines given in this document must still be followed.

The disclosure and transfer of personal data

21. Authorised and unauthorised disclosures

Staff members working with personal data will be made aware buy their line managers or other appropriate staff of the purposes for which the data is processed and the legitimate parties either within or outside appa training to whom that data, either in whole or in part, may be disclosed or transferred. Personal information must not be disclosed either orally

or in writing or via Web pages or by any other means, manual or electronic, accidently or otherwise, to any unauthorised third party.

22. Staff should note that unauthorised disclose will usually be a disciplinary mater, and may be considered gross misconduct in some cases

23. Security of data during transfer

Where personal data is transferred between staff members within the centre in the course of their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail in sealed envelopes or by hand. If transferred by e-mail, such data should normally either be encrypted or sent in a password-protected attachment (for example using Microsoft Words 'require password to open' feature), with the password being supplied separately. Further advice on secure email and password protection can be obtained from the appa IT support desk.

24. Disclosure outside the centre

When a request to disclose or amend personal data relating to a member of the centre (student or staff) is received from an individual or organisation outside the centre, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established. Disclosures requested by those claiming to be relatives or friends should be refused unless the consent of the data subject is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law.

25. Requests for the disclosure of personal data from the Police, Government bodies, the British Council or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

26. Details of any specific procedures and practices to be adopted when responding to requests for disclosure in individual administrative Departments within the centre will be available from the appropriate staff.

Publication of centre information

27. While the majority of personal data held by the centre is processed for internal administrative purposes and is never disclosed outside the centre, some categories of data are routinely or from time to time released through one or more forms of publication.

28. Legal obligations

When required by law, the names of senior staff of the centre and certain other personal data relating to employees are published on the web site. The centre also fulfils all obligations placed upon it by its relationships with various funding bodies, government agencies and the like with regards to the release of personal data and statistical information concerning students and staff. Data subjects are informed of the centres obligations in this respect at the time the data is collected.

29. Staff directory

In order to meet the legitimate needs of visitors and enquiries to be able to make contact with appropriate staff, the centre makes client names, positions and contact details available in its welcome packs. However, at the time of appointment and at any time whilst in post (via a request to the designated Data Controller) each individual member of staff will be able to specify the level of detail that will appear in these packs.
The web-based public directory will be searchable by name and organisational unit and will only return personal contact data for those staff that have given their consent for this disclosure

30. Staff personal data on web pages

Apart from the staff directory described above, staff biographical details or other personal data may be published on appa trainings web site or in other media, but only where the staff concerned have given their consent for such information to be made publicly available. However publication in this way does not mean that such data have been placed into the public domain. Centre retains control and copyright of such data, and the data must not be reproduced or further processed without the centres express permission.

31. Student personal data on web pages

Apart from the obligations mentioned above (paragraph 28) the centre will not ordinarily reveal any personal details of students enrolled at appa to any individual or body outside the centre.

Retention and Disposal of Personal Data

32. The retention of personal data

The centre has a duty to retain some staff and student personal data for a period of time following their departure from the centre, mainly for legal reasons, but also for other purposes such as being able to provide references and for financial reasons, for example relating to pensions and taxation. Some material will also be retained to form part of the official centre archive. Different categories of data will be retained for different periods of time, and these ae set out in the table overleaf.

33. The disposal of personal data

When a record containing personal data is to be disposed of, the following procedures will be followed:

- All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data
- All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-forming over-writing or degaussing.

34. Employees and, where appropriate, students, will be provided with guidance as to the correct mechanisms for disposal of different types of personal data and audits will be carried out to ensure that this guidance is adhered to. In particular, employees and students will be made aware the erasing / deleting electronic files does not equate to destroying them.

Minimum Retention Periods for Records Containing Personal Data

Type of record	Minimum retention period	Reason for length of period
Personnel files including raining records, notes of disciplinary and grievance hearings, and appraisal forms	6 years from the end of employment	References and potential litigation
	Certain personal data may be held in perpetuity	Selected material will form part of the official centre archive
Letters of references	6 years from the end of employment by the author of the reference letter	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where fewer than 20 redundancies	6 years from the date of redundancy	As above
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to when the records related	Income Tax (employment) Regulations 1993
Statutory maternity pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986
Statutory sick pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social security (claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	During employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	The Control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1958
Applicant records for those who are rejected or declined an offer	No more than 4 months after the start of the academic year	Permits institution to handle enquiries from the data subject
Student records of those not completing enrolment	Within one academic year	Permits institutions to handle delayed enrolments
Student records, including enquiries, applications, admissions, assessment, awards, attendance and conduct	At least 6 years from the date that the student leaves the centre, in case of litigation for negligence	Limitation period for negligence
	At least 10 years for personal and academic references	Permits institutions to provide references for a reasonable length of time
	Certain personal data may be held in perpetuity	While personal and academic references may be 'stale', some data e.g. transcripts of students marks may be required throughout the students future career. Upon the death of the data subject, data relating to him/her ceases to be personal data. Some selected material will form part of the official centre archive.

Subject Access Requests

35. All staff, students, applicants and other users have a right under the Act to access certain personal data being kept about them at appa, either on computer or in certain files. Any person who wishes to exercise this rights should complete the Subject Access Request Form in Annexe 1 and submit it to the appropriate designated data controller, who is:

36. The centre will make a charge of £15.00 on each occasion that access is requested, although the centre has discretion to waive this.

37. The centre will comply with requests for access to personal information as quickly as is practicable, as required by the Act, but will ensure that the information is provided within 40 days.

38. Students and former students should be aware that exam scripts are exempted from the subject access rules and copies will not ordinarily be given to those who make a subject access request. However, a copy of summary of both internal and external examiners comments can be requested as part of a subject access request. If such a request is made before the results of the examination are announced, the centre will provide the information within 5 months of the request being received or 40 days from the announcement of the results, whichever is the earlier, as required by the GDPR.

The processing of Personal Data within Specific Administrative Departments and Training Centre Departments

Activities involving the processing of personal data

39. Listed in the following sections are categories of activities carried out within each of the specified organisational units within the centre that involve the processing of personal data. It is the responsibility of the appropriate Directors and managers to ensure that sufficiently detailed guidance is given to their staff to enable them to carry out these activities in accordance with the requirements of the Data Protection Act 1998.

40. Faculties.

- Admissions administration
- Enquiries administration
- Events / conference administration
- Examination and marking administration
- Marketing
- Staff recruitment
- Publication activities (including advertising and Web site/s)
- Staff management (including performance, appraisal and development records, leave records, expenses records etc.)
- Student assessment activities
- Student records / administration / student support
- Supplier / order / invoice administration
- Systems administration (e-mail, back-up / storage, authentication, system logs etc)
- Teaching activities and administration
- Teaching performance / assessment / review activities

41. Central Computing Systems

- Staff management
- Staff recruitment
- Student registration
- Accounts
- Systems administration (MIS, e-mail, back-up/storage, authentication, system logs etc.)
- Telephone system administration
- Training records administration
- Web site forms
- Room bookings administration

42. Centre BSU services

- Archives
- Corporate planning and management activities
- Data protection SAR administration
- Governance activities
- Health and Safety activities and administration
- Staff management
- Staff recruitment
- Supplier/order/invoice/administration

43. Facilities

- CCTV
- Facility Management
- Security / access control systems and records

- Health and Safety activities and administration
- Telephone Operator activities

44. External Relations

- Events
- Fundraising activities
- Graduation ceremonies administration
- Mailing list administration and use
- Marketing
- Market research
- News / press release activities / public relations
- Staff recruitment
- Supplier / invoice / orders / administration

45. Finance

- Archives management
- Financial management and accounting
- Payroll administration
- Pension scheme administration
- Staff recruitment
- Student financial records administration
- Supplier / order / invoice administration

46. Human resources and staff management

- Archives management
- Data protection SAR administration
- Employee relations management
- Records of monitoring in accordance with the Race Relations Amendment Act 2000
- Staff development and support activities / administration
- Staff management (includes performance, appraisal and development record, leave records, expense records, etc.)
- Staff recruitment
- Online staff portal
- Supplier / order / invoice administration

47. Resources / Library

- Loan administration

48. Centre CEO

- Department daily and annual function
- Staff management
- Centre development and growth
- Centre standing / governance
- Teaching performance / assessment / review management
- Supplier/order/invoice administration

49. Registry (BSU)
    - Admissions administration
    - Archives management
    - Assessment administration
    - Awards administration and conferment
    - Data protection SAR administration
    - Enquiries administration
    - Students support activities
    - Student's records administration, including disability information
    - Teaching / assessment administration

50. Student Services
    - Social activities administration
    - Student records administration

51. Training Centre Managers Office
    - Overseeing all listed departments above
    - Student disciplinary activities
    - Teaching performance
    - Student support
    - Consultancy administration

Annexe 1

appa training

Subject Access Request Form

1. Details of the person requesting the information

Full name: _____

Address: _____

_____

_____

_____

Contact Number: _____

Email: _____

2. Are you the Data Subject?

☐ YES

If you are the Data Subject please supply evidence of your identity i.e. driving license, birth cert (or photocopy) and, if necessary, a stamped addressed envelope for returning the document. Please also state your relationships to appa training.

☐ I am a current/former member of staff

☐ I am a current/former student

☐ I am neither of the above

Please now go to question 5.

☐ NO

Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed. Please also state the relationship of the Data Subject to appa training:

☐ The Data Subject is a current/former member of staff

☐ The Data Subject a current/former student

☐ The Data Subject is neither of the above

Please now go to questions 3 and 4

3. Details of the Data Subject (if different from 1.)

Full name: _____

Address: _____

_____

_____

_____

Contact Number: _____

Email: _____

4. Please describe your relationships with the Data Subject that leads you to make this request for information on their behalf:

_____

_____

_____

_____

_____

_____

_____

_____

_____

5. If you wish to see only certain specific document(s) for example a particular examination report, a specific departmental file etc, please describe these below:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

6. if you would like a more general search, please note that the centre is able to search the following sections for personal date. Please indicate the sections that you would like searched:

☐ Registry
☐ Human Resources
☐ Finance
☐ Training centre / Facilities
☐ Other: _____

_____
_____
_____
_____

☐ Administrative Department files and information systems

7. Declaration

1,_____, certify that the information given on this application form is true. I understand that it is necessary for the centre to confirm my/the Data Subjects identify and it may be necessary for more detailed information to be obtained in order to locate the correct information.

Signed: _____

Date: _____

Please return the completed form to the appropriate Designated Data Controller at the address given below:

For students/former students: Student Support
For Staff/former staff: Human Resources or Line-Manager
For all Others: Training Manager

appa me Ltd, 2nd Floor, 307-313 Lewisham High St
London SE13 6NL

Documents which must accompany this application are:

- Evidence of your identity
- Evidence of the Data Subjects identity (if different from above)
- Evidence of the Data Subjects consent to disclose to a third party (if required as indicated above)
- A fee of £15 (cheque to be made payable to appa training)
- A stamped addressed envelope for return of proof of identity / authority documents, where appropriate.

Please note that the centre reserves the right to obscure or suppress information that relates to other third parties (under the terms of GDPR)

Office use only

Request received: _____
Date Completed: _____
Notes: _____