Data Protection Policy and Guidelines

The Data Protection Act and other associated legislation impose obligations, not only on Peterborough Skills Academy as an organisation but also on each member of staff individually. The legislation therefore affects you personally. This leaflet has been produced to give you information and advice on the requirements of the Act. It will help you fulfil your personal responsibilities.

Do not hesitate to seek further advice on any point you do not understand. It is essential to comply with the requirements of the Data Protection Act. Failure to do so may result in legal action against Peterborough Skills Academy or against you as an individual.

CONTENTS

Definitions	*Page*
1. The Principles	2
2. Security of Personal Data	3
3. Conditions for Processing	3
4. Information Gathering	4
5. Information Processing	6
6. Subject Access Procedures	6
7. Useful Reminders	8
8. GDPR Updates	9

DEFINITIONS

Within these guidelines, a number of terms are used which are explained below:

Personal Data:

Data which relate to a living individual who can be identified from the information, whether by name or by code (such as a reference number) which can be related back to a name. Examples of personal data are name, address, date of birth or any expression of an opinion about an individual.

Data Subject:

An individual who is the subject of personal data. For example: a council tax payer, a housing benefit recipient – or you, as a member of staff.

Data Controller:

A person or organisation who holds data and controls the contents or use of data.

Data Processor:

Any third party (other than the employee of the data controller) who collects and/or uses personal data on behalf of the Data Controller. This even includes those responsible for the disposal of any confidential waste.

Processing:

Amending, adding to, rearranging, deleting or extracting information from the data. In the context of the Data Protection Act "processing" means performing any activity data from collection to destruction.

Disclosure:

The communication of personal data to another organisation or individual.

Information Commissioner:

The government body responsible for the implementation and policing of the Data Protection Act 2018. They have the authority to both investigate and prosecute on behalf of any individual who believes their personal data is not being held in accordance with the Act.

Notification:

The Information Commissioner maintains a public register of data controllers. Each registry includes the name and address of the data controller and a general description of the processing. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller. Notification is the process by which a data controller's details are added to the register.

1. THE PRINCIPLES

PERSONAL DATA IS YOUR RESPONSIBILITY

The law says you must:

- Obtain and process it fairly and lawfully
- Use it only for a defined purpose
- Ensure it is adequate, relevant and not excessive
- Keep it accurate and up to date
- Delete it when no longer required
- Process it in accordance with the data subject's rights
- Keep it secure
- Not transfer it to other countries without adequate protection

2. SECURITY OF PERSONAL DATA

Every time Peterborough Skills Academy communicates information based on personal data, it must be to an organisation or person covered by the authority's appropriate Data Protection Act notification.

This means that everybody should guard against accidental disclosures by taking their personal responsibility seriously with respect to security.

Secondly, those responsible for systems should make themselves aware of all the regular, planned disclosures of personal data that are part of their system and check that they are notified - this can be done on-line at www.informationcommissioner.gov.uk

Thirdly, staff may, as part of their job, receive requests for information about personal data – by telephone, in writing, or face to face. It is vital in these circumstances that you satisfy yourself that Peterborough Skills Academy is notified to disclose to that type of person or organisation and that they really are who they claim to be.

When checking the identity of the enquirer explain why you need to do it and mention the Data Protection Act.

Examples of approaches to identification include:

- If on the telephone, ask for some information only the caller would know
- If in person, ask to see some proof of identity

If by letter, check that the return address is appropriate to the enquirer and, if you are in any doubt, you should ask for proof of identity to be sent.

IF IN ANY DOUBT DO NOT DISCLOSE PERSONAL INFORMATION. Seek advice from your manager or the departmental DP representative. Do not be intimidated into providing information immediately to the Police, the Inland Revenue or elected members etc. The Police and Inland Revenue are required to issue a Section 29 notice under the Data Protection Act and any approaches from other individuals or bodies should be referred to your manager. You are responsible for the personal data you process – take your responsibility seriously.

If the request is from a data subject about their own data, and it is in writing, then it may be a formal 'Subject Access Request' under the Act and should be referred to the DP representative or the Information Manager, who will action as necessary.

Ensure that computer screens that may display personal information are not visible to the public or other individuals who should not have access to the data.

Manual records containing personal data are now covered by the Act and should be kept in secure filing cabinets which are locked when not in use.

Introduce a clear desk policy which ensures that personal information is not left lying about.

Home-working and off-site visits need to be remembered when considering security of data.

3. CONDITIONS FOR PROCESSING

Conditions for processing personal data are as follows:-

- Consent of data subject
- Necessary for performance of contract with data subject
- Legal obligation

To protect the vital interests of the data subject At least one of these conditions must be met in order to process personal data.

There are further conditions which must be met before processing sensitive personal data. Sensitive data includes:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health condition
- Sexual life
- Criminal offences
- Criminal proceedings/convictions

Before processing sensitive data at least one different condition must be met from the following:- Explicit consent of the data subject

- To comply with employer's legal duty
- To protect the vital interests of the data subject or another party
- Information has been made public by the data subject
- In legal proceedings

- Exercising legal rights
- To carry out public functions
- For medical purposes
- For Equal Opportunities monitoring

As specified by Order One of these conditions must be met before processing takes place. Consent of the individual can be by way of an application form or verbal consent. Explicit consent must be obtained prior to publication of personal data on the Internet. E-mail address, photograph or any information which identifies an individual constitutes personal data.

Where children's data are likely to be published on a school web site the parent's/guardian's explicit consent must be obtained.

If information is received from a third party the data subject must be made aware of this if at all possible.

4. INFORMATION GATHERING

All forms used to obtain personal data, such as registration forms or application forms, either on paper or over the Internet, should state the purpose for which they are being obtained and make appropriate use of the 'padlock' symbol.

The initial obtaining of data about an individual is an absolutely vital process in data protection terms, and the way it is done can affect the legality of all future processing of personal data.

The essential requirement in this process is that the individual must be in no doubt why the personal data are being collected. It is the responsibility of the authority and any member of staff personally involved in information-gathering activities to ensure that the reasons for collecting the personal data are clearly explained.

As it may require a specific form of words it is recommended that you speak to your DP representative or the Information Manager before embarking on new initiatives in these areas.

Arrangements with external organisations/partnerships must ensure that Data Protection compliance is included in the contract/agreement.

5. INFORMATION PROCESSING

Processing of personal data must meet the conditions for processing as detailed in Section 3 of this leaflet.

Before creating your own local file of personal data remember that it must be in accordance with the Data Protection principles. First, consider the purpose for which you are using the personal data:

- Is the purpose registered?
- Is it consistent with the original purpose for which the data was obtained or would the data subject perceive it as unfair?

You can use other Data Protection principles as helpful checklists to assess the effectiveness of your local file of personal data:

- Is the personal data 'relevant and not excessive'? In other words does all the information really contribute to your purpose?
- Is the information 'accurate and up to date'?
- Does the system allow you to correct inaccuracies and/or delete personal data which should not be on your file?

Have you a way of regularly ensuring that you will 'delete it when no longer required'? 'Subject Access Right' is a good test of your openness – remember data subjects have the right to a complete print out (or a complete copy, in the case of manual files) of all the personal data held about them. You should therefore only hold personal data that you would be prepared to let the data subject see.

You must inform your manager of any such file containing personal data so that an audit form can be completed, detailing the contents, which will then be added to the authority's Data

Protection database. Remember to follow this procedure for any amendments, deletion or destruction of the information held.

Finally, all files containing personal data must be kept secure:

- Don't let unauthorised people see personal data on your screen or on file unless they really need to do so for a valid business reason
- Dispose of paper with personal data on it as confidential waste
- Lock away personal data held in any format
- Don't discuss personal data in public places where you can be overheard

ALL systems and files containing personal data must comply with these conditions.

Destruction of Personal Data

Destruction of manual files containing personal data must be by shredding. If an outside contractor is used, ensure that Data Protection compliance is contained in the contract. Redundant computer equipment must be disposed of through ICT, whether or not personal data is held on the equipment.

System Development

For new systems the Data Protection principles should be built into the system. This means thinking about all the purposes for which personal data in your system will be used and checking all the data classes and recipients are registered.

Think about accuracy checks; perhaps you could include in the overall system design an annual mailing to all the individuals the data pertains to, so they can correct it if necessary. In any event, design an easy way for correcting errors in the basic data.

Think about obsolescence; are there any measures you can build into the system to prevent the build-up of obsolete personal data? Perhaps a specific reminder, or procedure, every six months for users to indicate which data can be deleted.

All systems with personal data must have a capability of responding to Subject Access Requests – a comprehensive print out of all data relating to an individual, including translations or explanations of coded data.

The Act applies equally to personal data used for testing. Where possible, test files of personal data should be de-personalised.

Retention Periods

The sixth principle requires that *"personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".* To comply with this principle, it will be necessary to review regularly the personal data held and delete those which are no longer required. Consult the Retention Guidelines, held on the Intranet.

6. SUBJECT ACCESS PROCEDURES

Any individual is entitled, on making a written request, to be supplied with a copy of any personal data held about them. In nearly all circumstances such a request – known as a 'Subject Access Request' – must be responded to within 40 days.

There are two points in the subject access process where you are likely to become involved. They are:

- Receiving a subject access request
- Searching for and listing personal data

The following sections deal with these areas in more detail.

Receiving a Subject Access Request

You must be alert to the possibility of receiving a subject access request. The important thing is to differentiate between general requests for specific pieces of information (eg. about an individual's council tax benefit) and broader requests asking for complete listings of data held. Bearing in mind that a formal subject access request must be in writing, you should therefore look out for the following indicators of such a request:

- The letter refers to Data Protection
- The letter asks to see data (rather than information), providing a clue that the request is more significant than just a casual enquiry
- The letter says, or intimates that, the writer wishes to see 'all of the information', or 'complete lists', suggesting a wide-ranging enquiry

If you believe you are in possession of a subject access request, do not acknowledge it, but send it straight to the Information Manager who will deal with it as appropriate.

Searching for and Listing Personal Data

The Information Manager will be managing all subject access requests and may ask you to search for all personal data on an individual data subject.

The Information Manager will clearly indicate that it is part of a subject access request and will describe what you are required to do.

As there is a legal maximum response time for subject access requests, it is vital that you action the request quickly and accurately. You will be required to list all personal data held on the data subject in question and to explain any 'coded' data. It will be your responsibility to ensure that:

- All files and systems (including PCs) in your area which might contain personal data about the individual are properly searched

- All records relating to the individual are printed out or copied accurately, completely and without being changed in any way. **Note: The Act expressly forbids any amendment or deletion of personal data as a consequence of receiving a subject access request.**

The Information Manager will then use this information as the basis for responding to the data subject. The Information Manager will contact you again if further interpretation or explanation of the personal data is required.

7. USEFUL REMINDERS

Peterborough Skills Academy wants to emphasise great importance to these basic rules which have been drawn up to protect the interests of the authority, the public and YOU.

ALWAYS work strictly within Peterborough Skills Academy's Data Protection Staff Guidelines and the Data Protection principles. If, as part of your job you collect personal data you must:

- Obtain the personal data fairly and lawfully

- Only collect the personal data for valid and notified business purposes

- Only collect the personal data if it is really necessary for the purpose(s)

- Make sure the personal data is accurate

- Ensure the person providing the information (normally the data subject) clearly understands the purpose(s) for which the information will be used

- **NEVER** disclose any personal data to anyone not entitled to see it:

- **ALWAYS** satisfy yourself that Peterborough Skills Academy is registered to disclose personal data to them

- **ALWAYS** do whatever is necessary to confirm their identity before doing so

- **NEVER** disclose personal information during casual conversation or allow business discussions to be overheard by third parties not entitled to the information.

- **ALWAYS** correct inaccurate personal data – or report it to someone who can

- **NEVER** record any information about an individual that you would not be prepared to let them see
- **NEVER** leave computer print-out lying around when not being used. Lock work files away before leaving your workplace at the end of the day

- **NEVER** take computer print-outs home to be used as scrap paper

- **ALWAYS** dispose of personal data as confidential waste

- **ALWAYS** be careful if you take personal data outside Peterborough Skills Academy's normal office environment

- **ALWAYS** keep access to your password secure

- **NEVER** make your password available to anyone else

- **ALWAYS** satisfy yourself that any personal data you store is relevant and not excessive for the business purpose(s) for which it is held and registered

- **NEVER** store personal data for any longer than is really necessary for the purpose(s). Review the data at regular intervals and delete it in line with the Retention Guidelines

- **ALWAYS** ensure appropriate controls are in place to prevent unauthorised access

- **ALWAYS** sign off when you have finished

8. **GDPR – Data Protection Policy**

Peterborough Skills Academy is fully committed to prepare for and, after 25 May 2018, to comply with the General Data Protection Regulation (GDPR). The GDPR applies to all Colleges that process data relating to their employees, as well as to others including customers, contractors, and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed.

To this end, Peterborough Skills Academy endorses fully and adheres to the six principles of data protection, as set out in the Article 5 of the GDPR.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
5. Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or Collegial measures.

These principles must always be followed when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Business will:

- Observe fully the conditions regarding the fair collection and use of information including the giving of consent
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the information is held for no longer than is necessary
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to access one’s personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- Take appropriate technical and Collegial security measures to safeguard personal information
- Publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection

- Ensure that personal information is not transferred abroad without suitable safeguards.

Scope and Status of this Policy

All staff:
The Policy does not form part of the formal contract of employment for employees, but it is a condition of employment that employees will abide by the rules and policies of the Business. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings.

Designated Data Protection Officer:
The Designated Data Protection Officer (DPO) [the Personnel Manager] will deal with day-to-day matters. Any member of employees, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the DPO.

Employee Responsibilities

All employees are responsible for:

- Checking that any information that they provide to the Business in connection with their employment is accurate and up to date
- Informing the Business of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently.
- The Business cannot be held responsible for any errors unless the employee has informed it of such changes.

Data Security

All employees 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.

Employees should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe. Advise the DPO of any data breaches as soon as possible.
Personal data breaches will be required to be communicated to the ICO by the DPO

'without undue delay' and in any event within 72 hours of the breach being identified unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects. The breach report will need to include:

- The nature of the breach, including an approximate number of data subjects involved and the categories of personal data affected
- The likely consequences of the breach
- The measures taken or proposed to address the breach and measures being taken to mitigate the stated consequence

The Business will also communicate to all affected data subjects without undue delay (unless the breach is unlikely to result in a high risk to the right and freedoms of the data subjects). There are circumstances where such communications is not required:

- Where general measures (technological and organisational) have been adopted to render the personal data as unintelligible to any person not authorized to access it. Eg through encryption or robust password protections.
- Where subsequent actions have removed the risk of the rights or freedoms of data subjects beyond likelihood Where such communication would be one of disproportionate effort providing that the College makes an appropriate public statement instead so that data subjects are informed in an equally effective manner.

Disaster Recovery

1. PSA backs up data every day and has multiple copies (at least one set for each day of the week and additional weekly ones in order to have at least a month's worth of data at any one time). Records of these are kept.
2. Backups are kept on site are in special heat-proof safes: fire-proofing alone is inadequate.
3. Backups are verified regularly by the software and system supplier.
4. Firewalls and virus checkers are kept up to date and running, and users are trained in virus avoidance and detection.
5. Computers are protected from physical harm, theft or damage, and from electrical surges using protective plugs.
6. PSA plans for how to deal with loss of electricity, external data links, server failure, and network problems. It uses paper forms where necessary for temporary record keeping.

Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre- ticked boxes nor any other method of default consent is allowed. As required by the GDPR, the Business takes a "granular" approach ie it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the Business ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following:

- Contract: if processing someone's personal data is necessary to fulfil the Businesses contractual obligations to them (eg to provide a quote).
- Legal obligation: if processing personal data is necessary to comply with a common law or statutory obligation.
- Vital interests: not one that will occur often as it refers to processing personal data to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent.
- Legitimate interests: the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Subject Access

An employee may request details of personal information which the Business holds about him or her under the GDPR. A small fee may be payable and will be based on the administrative cost of providing the information. If an employee would like a copy of the information held on him or her, they should write to the Data Protection
Officer at Peterborough Skills Academy, PE1 5FQ. The requested information will be provided within one month. If there is any reason for delay, that will be communicated within the four week time period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).
If an employee believes that any information held on him or her is incorrect or incomplete, then they should write to or email the Data Protection Officer at PSA Training as soon as possible. The Business will promptly correct any information found to be incorrect.

Right to be forgotten

PSA Training recognises the right to erasure, also known as the right to be forgotten, laid down in the GDPR. Individuals should contact the Data Protection Officer with requests for the deletion or removal of personal data. These will be acted on provided there is no compelling reason for continued processing and that the exemptions set out in the GDPR do not apply. These exemptions include where the 0000personal data is processed for the exercise or defence of legal claims and to comply with a legal obligation for the performance of a public interest task or exercise of official authority.