Protocol Consultancy Services

Data Protection Policy (GDPR), including Key Procedures

ISSUE:	20
DATE:	May 2020

Contents

Aims of this Policy

This section explains:

- why data protection is important to Protocol
- the legal basis for the policy
- general aim of this policy
- who in Protocol needs to comply with this policy and key procedures

The Data Protection Act applies to all organisations processing personal data.

Protocol Consultancy Services needs to keep certain information on its (employees, employers, sub-contractors, service users and learners) to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

Protocol is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 2018 and GDPR. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within Protocol.

This policy covers: -

- Staff
- Employers
- Parents
- Learners
- Sub-Contractors

Definitions

In line with the Data Protection Act 2018 principles, Protocol will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. Protocol will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.

- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.

- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.

- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.

- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of information processed

There are different types of information used by Protocol and include:

- Information on applicants for traineeships and apprenticeships jobs, including references
- Employee information – contact details, bank account number, payroll information, supervision and appraisal notes.
- Parents financial information
- Sub Contract learner information
- Employer details

We keep information in paper based and computer based systems.

Particular consideration must be given to how sensitive personal information is kept within Protocol. i.e. information about ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions and this is stored on the confidential information records.

Notification

Protocol will comply with the legal requirement to 'notify' the Information Commissioner that personal data is being processed .There is a direct debit set up that comes out of the account of Transworld t/a/ PCS annually.

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Susan Tipton.

The Act has seven parts.

- This Act makes provision about the processing of personal data.
- Most processing of personal data is subject to the GDPR.
- Part 2 supplements the GDPR and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply.
- Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive.
- Part 4 makes provision about the processing of personal data by the intelligence services.
- Part 5 makes provision about the Information Commissioner.
- Part 6 makes provision about the enforcement of the data protection legislation.
- Part 7 makes supplementary provision, including provision about the application of this Act to the Crown and to Parliament.

Responsibilities

Protocol will meet its responsibilities under the policy as follows:

To meet our responsibilities staff will:

Ensure any personal data is collected in a fair and lawful way;

- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.

Queries about handling personal information will be dealt with swiftly and politely.

Training

Protocol requires that people handling personal data are suitably trained.
On induction:

- Through the Staff Handbook and listed policy & procedure documents.
- Recipients sign for information received as proof of receipt and understanding
- Other information we provide e.g. re not disclosing passwords, keeping files locked and location of keys and codes private

Awareness raising:

- We regularly update the staff handbook and refer to the DPA in training as an update for staff minimum annually.

Gathering and checking information

Protocol has also reflect on the following and has considered

- What details are necessary and for what purposes
- How long we are likely to need this information

We also explain how we inform people, before they give us information, about:

- why the information is being gathered
- what the information will be used for
- who will have access to their information (including third parties)

(in most cases, this is simply stated on the form that they complete)

There are specific requirements for personal sensitive information. Consent must be sought each time it is to be used. This is information about ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions etc. The information will have been captured for a specific purpose- e.g. to explain absence. If we need to use the information for another purpose, even a related purpose, this will require specific consent.

We will inform people whose information is gathered about the following:
The need to share with the Education Skills Funding Agency if they are on government funding programmes and their agents and Ofsted

We will take the following measures to ensure that personal information kept is accurate through reviews and IAG sessions.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

Data Security

Protocol will ensure the security of the personal data held. Unauthorised disclosures can lead to criminal prosecutions and know how important it is to set out how data should be protected e.g. how personal information is protected from unauthorised people viewing it and from loss (including computer documents, emails and paper copies):

- Lockable cupboards (restricted access to keys)
- Password protection on personal information files
- Setting up computer systems to allow restricted access to certain areas, permissions across the I Drive to selected staff members
- Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick), only 4C not the main file
    - Only at sign up stage can information be taken off site for completion purposes, but must be returned straight to the office to minimise risk
- Back up of data on computers is completed via the server and remote backups completed and data given to the MD
- Personal information is not allowed to be stored on staff desktops or local hard drives, all information must be stored onto the I Drive or approportionate server share.
- Any Information Security Incident or Data Breach affecting any stakeholders will need to be reported immediately.

The MD is accountable for compliance of this policy and staff may be subject to disciplinary procedures if they are found to be in breach of the company requirements.

Protocol will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action.

Subject Access Requests

Those who have personal data being processed by Protocol can request access. This is a right under the DPA and the policy spells this out quite clearly.

Information that will be required by Protocol before access is granted. The type of information will typically include:

- Full name and contact details of the person making the request
- Their relationship with Protocol (former/ current member of staff, trustee or other volunteer, service user
- Any other relevant information- e.g. timescales involved
- Type of identification required before releasing any information (e.g. passport, birth certificate etc)

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the MD Susan Tipton. We may also require proof of identity before access is granted. The following forms of ID will be required passport/driving licence.

Queries about handling personal information will be dealt with swiftly and politely.
We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 10 days required by the Act from receiving the written request.

Review

This policy will be reviewed annually to ensure it remains up to date and compliant with the law.

Declaration

I confirm I have read and understood Protocol's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

- ☐ Member of staff

Signature:
Print name:
Date:

Please return this form to S Tipton MD.
See also the separate GDPR Policy