DATA PROTECTION POLICY

Contents

Date	Document Version	Draft / Final	Distribution	Comment
Feb 2017	1.0	Final	All staff	Initial Document released

Definition of “data” and “data subject”

When this policy refers to “data”, this applies to any personal information kept by the organisation for the purposes of processing. A “data subject” is a client, worker (employee, volunteer, placement student or agent temp) or other person or organisation that we may hold records on or communicate with.

Where generalised, the policy also includes business sensitive information.

Aim

- Ensure compliance with the Data Protection Act 1998, including the eight main principles:
    - Fairly and lawfully processed
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate and up to date
    - Not kept for longer than is necessary
    - Processed in line with your rights
    - Secure
    - Not transferred to other countries without adequate protection
- Ensure the rights of a data subject to access their personal data that the organisation holds while protecting the rights of third parties
- Guide specifically on the use of references State retention periods for each type of data.

Files

Filing systems should be kept in a way that respects the information held:

- Data must be kept in a lockable filing cabinet or other secure storage compartment.
- Workers must ensure that such data is not left in the sight of others and is filed when not in use.
- Any changes to personal data, such as a new address, should be carried out at the first available opportunity to minimise the risk of information being misdirected.
- Checks to ensure correct personal details should be made where a client reopens their case or a worker returns to the organisation after leaving.

Electronic data

Enter-at will ensure that all electronic data, including client database entries, emails and letters are accessed and secured by minimum of the following;

- Strong strength passwords
- Up to date anti-virus, anti-spyware and firewall software to prevent unauthorised access via means of malware, viruses / Trojans
- All laptop equipment is supplied with encryption software.
- In line with the ICT policy, workers are to keep passwords confidential. In extreme cases where it is necessary for the password to be shared, immediate steps should be taken to change the password.

As official documents, emails to any Enter-at account may be accessed in the absence of the account holder by their manager or as part of a Data Protection Access Request through the ICT department. Subject to an official request, emails may also be monitored for the purposes of quality and monitoring performance or as otherwise specified in the Enter-at ICT Policy.

Revealing data to third parties

Data must not be revealed to a third party without the data subject's consent. This would only be breached in line with the levels of breach contained in the Confidentiality Policy or in issues relating to national security.

Where a third party is in another country, data will only be revealed where equivalent data protection laws exist or where a contracted agreement with the third party is accepted by the client and by Enter-at.

TUPE

In the event of a loss of an existing contract or a new contract bid is successful, the terms of the contract may stipulate that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (commonly known as TUPE) apply. In this situation, Enter-at is obliged to share/receive specific data about workers under these terms.

Transfer of Client Data

Whether TUPE regulations are in place or not, Enter-at must work with the organisation involved in a transfer of client data, to gain consent from clients before that data is shared with or received from them. Clients will receive written notice that a change is taking place and that they have the right to refuse their data being transferred.

Security breaches

Enter-at must report security breaches to the Information Commissioner (ICO) if it is believed that data is at risk of being misused as a result of loss of data. All possible breaches will be recorded by Enter-at. In line with the ICT policy, it is the employees' responsibility to inform the loss or possible loss of data to:

- Resources Manager
- Director of Enter-at

Data Protection Requests

Data subjects have the right to access personal data which is held by the organisation, both files and electronic data. Guidelines are in place to ascertain whether an official Data Protection Request Procedure is needed or not.

If an official request is needed, Enter-at has 40 days to reply to such requests. A fee of up to £10 is chargeable for copies of paper records holding such information.

When fulfilling the request, Enter-at must take into consideration any data that has third party involvement. Data can be withdrawn if:

- The third party has not given consent for the data subject to see the data
- The data would lead to the harm of the data subject or third party For

  more information, please see:

- Subject Access Request Form
- Subject Access Request Procedure and Guidelines
- Subject Access Response Form
- Subject Access Withdrawals Form

On the occasion that a relative, solicitor or other third party makes a subject access request on a subject's behalf, either because the subject lacks capacity or is deceased, Enter-at will require evidence that such a person is formally acting on their behalf. Such requests will be reviewed on a case by case basis to determine whether such data can be released to the third party.

Requests for copy of electronic files held

For copies of electronically held data Enter-at will require an official request to be made,

References

All references given by an Enter-at worker should remain factual and should resist giving opinions of the referee or other staff members which cannot be backed up by evidence. Former or existing workers cannot request to see these references from Enter-at but can apply, under the Data Protection Act, to request these from their new employer.

Subsequently, workers have the right to see references about them that are held by Enter-at.

Data Protection Audit

An audit of current data, both manual and electronic must take place annually on or around:

- June for Client Records
- September for Worker Records

This will involve checking whether the data should still be kept under the retention periods stated on the next page. When data is due to be destroyed after it has reached the end of its retention period, this should be done so that the document cannot be used again (ie. files are shredded, computer files and database entries are deleted).

Managers must then report back to the Data Protection Officer to confirm this has been done for their office/project.

Retention Periods

Enter-at adheres to the statutory retention periods for worker, financial and health and safety data. Examples are outlined below:

Record	Retention period	Archiving period	Action
accident books, accident records/reports	12 years for records relating to accident or injury at work	None	Destroy
accounting records	2 years	4 years	Destroy
income tax and NI returns, income tax records and correspondence with the Inland Revenue	2 years after the end of the financial year to which they relate	4 years	Destroy
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	2 years after the end of the tax year in which the maternity period ends	4 years	Destroy
Statutory Sick Pay records, Calculations, certificates, self certificates	2 years after the end of the tax year to which they relate	4 years	Destroy
wage/salary records (also overtime, bonuses, expenses)	2 years	4 years	Destroy

Enter-at also holds other data where the following retention period applies:

Record	Retention period	Archiving period	Action
Client files	18 Months after the closure of the file	None	Destroy
Worker records	6 years after the worker has left	4 years	Destroy
Grievance/disciplinary records	1 year from end of employment	5 years	Destroy
Application forms and interview notes	Duration of employment for successful application and 6 months for unsuccessful applicants	None	Destroy
Electronic timesheets/ leave requests	3 years	None	Destroy
Meeting minutes (Board, EMT, SMT and Team)	3 years	Indefinitely	Archive store
Supervision notes	6 years after the worker has left	4 years	Destroy
Emails Employee personal mailbox	1 year	2 years	Destroy
Emails (Enter-at Core Depts, Sales, Support, etc)	1 year	4 years	Destroy
Exceptional files*	6 years	Indefinitely	Archive store

* Exceptional files include, but are not limited to criminal, investigational or national security data that are specifically excluded for these purposes.