Impact Initiatives Human Resources Policy	Procedure No: HR22/HJL
Data Protection	Page: 1 of 14
	Issue No: 1
	Date issued: March 2012
	Last reviewed: May 2018

Introduction

Impact Initiatives is required to collect and process certain personal data on individuals for the purposes of operational and legal obligations. The organisation recognises the importance of the correct and lawful treatment of personal data. We follow the regulations set by the Information Commissioners Office (ICO) which ensures we process data fairly and lawfully.

Training in data protection will be provided for all Impact staff and relevant volunteers so they understand the principles of data protection and are able to meet the expectations and legal obligations.

The types of personal data that the organisation may require include information about: current, past and prospective employees; volunteers, clients, suppliers and others with whom it communicates. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified by the Information Commissioners Office (ICO) in the General Data Protection Register (GDPR) which replaces the Data Protection Act 1998.

All information held and processed by anyone within Impact will adhere to the eight principles of the GDPR. These specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. These state that it must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes and not in a manner incompatible with these purposes;
3. Adequate, relevant and not excessive;
4. Accurate;
5. Not kept for longer than is necessary;
6. Processed in accordance with the data subject's rights;
7. Secure;

8. Not be transferred to a country outside the European Economic Area, without adequate protection.

1. Satisfaction of Principles

In order to meet the requirements of the principles, the organisation will:

- Observe fully the conditions regarding the fair collection and use of personal data;
- Meet its obligations to specify the purposes for which personal data is used;
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- Ensure the quality of personal data used;
- Apply strict checks to determine the length of time personal data is held;
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised under the Act;
- Take the appropriate technical and organisational security measures to safeguard personal data;
- Ensure that personal data is not transferred abroad without suitable safeguards.

Data Security

The need to ensure that data is kept securely means that precautions must be taken again physical loss or damage, and that both access and disclosure must be restricted. All employees and volunteers are responsible for ensuring that:

- Any personal data which they hold is kept securely;
- Personal information is not disclosed either verbally or in writing or otherwise to any unauthorised third party.

2. Core principles of data protection which all Impact employees and individuals must comply with are:

Legal collection of data

Any data collected must be within the six legal reasons listed in Appendix 1.

Secure storage of information

Impact has carried out a privacy impact assessment and risk assessment which list what data is processed and how the risks associated with this are minimised (Appendix 4).

Paper files and papers containing data as defined below in Appendix 2 must be stored in locked filing cabinets or drawers in offices which are locked when unattended.

Paper files requiring offsite storage will be kept to a minimum and e.g. mobile staff will be provided with lockable secure file storage boxes to maximise protection.

Electronically stored information must be kept only on equipment provided by Impact Initiatives unless clearly agreed otherwise with a senior manager and the IT and Facilities Manager.

Documents stored on individual hard drives or servers including Office 365 which contain identifiable data should be password protected.

Passwords allocated by Impact must always be used and screensavers set up must not be changed. Computer screens must be placed so they cannot be seen by any visitors to the office or any other person the information is not relevant to. Particular care must be taken if working in public spaces.

Electronic storage will be limited to as few devices as reasonable e.g. stored on a server or shared site rather than on disparate hard drives. This will ensure robust and effective management of data storage and disposal

Secure sharing of data

Any data to be shared electronically must be sent through encryption software or on a password-protected document with the password provided separately.

Documents for external meetings should be emailed to a person at the venue who is entitled to access the information for printing rather than physically carried to the venue.

In circumstances where there is no option to share documents electronically they should be sent through the post marked ‘confidential for addressee only’. This will be with recorded consent from the data subject

Subject Access requests

Impact will ensure all those we hold data on are aware that they have a right to see the data at any time and what the process for this is. Requests should be sent in writing to the Data Controller, after which information will be made available within 30 days. A small charge may be made for this.

Disposal of data

All data will be disposed of/deleted as listed in the timescales outlined below in Appendix 3 and the Data Retention Policy

All paper data records will be shredded on site or through the contracted secure service.

Electronic data held will be irretrievably deleted from devices.

Consent and communication

Impact will include clear, concise privacy statements on all documentation requesting data. This will include:

- What data will be held;
- The purpose for which the data in question is being processed;
- The recipient or class of recipient of the data in question;
- Any information available to the data controller pertaining to the source of the data in question.

Additional consent from the data subject will be required for sharing data with external personnel.

Designated Data Controller

The CEO is the Data Controller and responsible for ensuring compliance with the GDPR and implementation of this policy. Any questions or concerns about the interpretation or operation of this policy should be taken to the Line Manager or the CEO.

Photography, video and film

- **CCTV**

  CCTV will be used which solely for security purposes:

  - The cameras will be set up to capture only images on our property;
  - A notice will be displayed stating that cameras operate, why and that footage may be passed to the police
  - All staff with access to the footage will have clear understanding of how it must and must not be used and access to footage will only be available to those who need it;
  - No footage should ever be streamed or uploaded to a public site.

- **Photography and video**

  Written consent must be obtained prior to any photography or video of staff, volunteers or clients. This must state the purpose of the photographs and also how consent can be withdrawn at a later date should the person wish to do so.

Data breaches

A breach may occur if there is a deliberate attack compromising the integrity of the organisation. But a breach can also occur if there is an unauthorised access within the organisation or an accidental loss of integrity.

Not every incident relating to a lapse in security or integrity of a service is a breach. If there is no harm caused, or there is only a minimal effect resulting, this

will not qualify as a breach. However, a review of security measures will still be undertaken.

Staff and volunteers must immediately report the loss or possible loss of data to their line manager or other Impact manager in their absence. All possible data breaches will be recorded and by law must be reported to the ICO within 24 hours of the breach being identified. Information on how to report a breach is available at www.ico.org.uk. No breach should be reported without consulting the Data Controller.

3. Data processing

Impact will ensure that all those involved in processing data are familiar with the essential definitions used in Data Protection, which are:

Consent

Consent means offering individuals real choice and control. Genuine consent puts individuals in charge and builds trust and engagement.

Consent to process information can be given by the person if they are:

- Aged 11 plus – if under 11 years of age a parent or legal guardian must give consent;
- An adult who does not give reason to believe that they lack the capacity to agree to consent.

Personal data

The GDPR applies to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Anonymised data is not regulated by the Act unless, using other information you hold, it is possible to re-identify the individuals involved.

Processing

This means obtaining, recording or holding data, or carrying out any operation or set of operations on the data including:

- Organisation, adaptation or alteration of the data;

- Retrieval, consultation or use of the data;
- Disclosure of the data by transmission, dissemination or otherwise making available;
- Alignment, combination, blocking, erasure or destruction of the data.

Processing applies from the moment data is obtained to the moment it is destroyed and covers everything in between, including storing, collection, printing, reading and destruction of data.

Data controller

A person who determines the purposes for which and the manner in which any personal data is, or is to be, processed.

Data subject

An individual who is the subject of personal data, for example, employees or clients.

Data processor

A person who processes personal data on behalf of the data controller. This can include outsourced data processing functions, for example external payroll or healthcare providers, as well as anyone internally who deals with personal information about colleagues and customers.

Sensitive Personal Data

We process sensitive personal data solely for monitoring equalities and diversity or for the provision of specific services to individuals. This information must, as far as possible, be anonymised.

Sensitive personal data is defined as personal data consisting of information as to one or more of the characteristics listed below:

- Race or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexuality;
- The commission or alleged commission of any offence.

There are 19 conditions for the lawful processing of sensitive personal data which are set out in the Act and in secondary legislation. The most important of these are:

- The explicit consent of the data subject;
- The vital interests of the data subject;
- Equality of opportunity for ethnic minorities monitoring;
- In connection with seeking legal advice;
- Compliance.

Staff sickness records are also classed as sensitive personal data and therefore need to satisfy the legal obligation

4. Status of the Policy

Any breach of this policy will be taken seriously and may result in disciplinary action. Any employee, volunteer, or client who believes that the policy has not been followed in respect of their own personal data should raise the matter with their line manager or the CEO.

Appendix 1

Collection of Personal Data

We process personal data, including sensitive personal data, about all employees, volunteers, applicants for employment, relief workers, trustees, service users, self-employed contractors and others who work for us.

At least one of the six legal reasons must apply whenever personal data is processed.

These are:

- **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **(d) Vital interests:** the processing is necessary to protect someone's life.
- **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix 2

Any documents containing personal information on clients, staff and volunteers should be stored as described in the table below.

Document	**Storage**
Referral forms	Locked filing cabinet or drawer
Job application forms	Locked filing cabinet or drawer in a personnel file once successful Locked filing cabinet in date order file if unsuccessful Shared folder on Office 365 for shortlisting access
Health history/declaration forms	Locked filing cabinet or drawer in a personnel file once successful Locked filing cabinet in date order file if unsuccessful
Offending history	On application form so stored as above
DBS information	In Central Services Coordinator's email until start in job
Next of Kin forms	In locked filing cabinet
Incident forms	In locked filing cabinet
Accident forms	Locked filing cabinet in date and alphabetical order
Housing benefit forms	In locked filing cabinet
Bank detail forms	In personnel file in locked filing cabinet Staff database
Supervision or individual staff meeting notes	In locked filing cabinet
Team meeting notes	In locked filing cabinet
Communication books	Closed on central desk and in locked drawer when office is unattended
Transport lists	In locked filing cabinet or electronically
Sickness records	Password-protected electronic document

Appendix 3

Timescales for disposal of data held

The Data Controller holds overall responsibility for maintaining these timescales which refer to both paper and electronic data held. This is delegated as described below:

(L = Legal / D = Discretionary)

Data	Timescale	Responsibility	L or D
Staff and volunteer application forms	1 year after leaving (Summary record must be kept as below)	Central services Coordinator	L
Application forms of unsuccessful applicants	6 months	Central services Coordinator	D
Summary record of service	10 years after employment ends	Central Services Coordinator	L
Payroll and tax information	6 years	Finance Manager	L
Sickness records	3 years	Central Services Coordinator	L
Annual leave records	3 years	Central Services Coordinator	L
Individual staff meeting notes	1 year	Line manager	D
Unpaid or special leave	3 years	Central Services Coordinator	L
Annual appraisal records	5 years	Central Services Coordinator	L
Records relating to promotion, transfer, training, disciplinary matters	1 year after end of employment	Central Services Coordinator	L
Incident forms	3 years	Central Services Coordinator	
References given	5 years after end of employment	Central Services Coordinator	L

Data	Timescale	Responsibility	L or D
Records relating to accidents or injuries	12 years	Central Services Coordinator	L
Safeguarding	7 years after last contact If a member of staff is implicated data needs to be kept up to their 65th birthday or for ten years whichever is longest	Safeguarding lead	L
Client referral forms in and out of the organisation	Up to 2 years after end of service	Service manager	D
Information regarding clients to and from other organisations	Up to 2 years after end of service	Service Manager	D
Notes from client meetings	Up to 2 years after end of service	Service Manager	D
Electronic client data including emails	Up to 2 years after end of service	Service manager	D
Counselling records	3 years from end of service	Service Manager	D
Agreements with clients	Up to 2 years after end of service. A basic information sheet may be kept for longer eg. Name and dates involved in service.	Service Manager	D
Registers of attendance	3 months but retain numbers/anonymised data logged for monitoring purposes if required e.g. 3 new attendees, 40 in total attended	Service Manager	D
Transport lists	1 month	Service manager	D
CCTV footage	28 days	Service Manager	D

Exceptions

At times it may be reasonable to keep client information for longer than the timescale stipulated above for example if a client is likely to return to the service and the information would be conducive to providing a service in the clients best interests.

This is permissible if it adheres to the principle of shall not being kept for longer than is necessary for the purpose or purposes it was given and consented for.

Appendix 4

Risk	Mitigation	L	S	Level
Information shared inappropriately by Impact staff, volunteers or service users	• Clear guidelines given to staff volunteers and service users • Procedures and policies in place • IT devices set up appropriately • Staff and volunteer training • Relevant equipment provided eg. lockable filing cabinets • All aware of how their information can be shared • Confidentiality agreed at beginning of specific group sessions • Limited information taken off premises eg emailed to where a meeting will be held wherever possible • Relevant documents passworded or sent encrypted by email • Databases made to be secure with limited access • IT manager and CEO able to change access permissions to online documents or databases. Newman Business Solutions are also able to excluded staff from Office 365 or from remotely accessing Central team servers. • Use of Office 365 OneDrive – documents are kept within OneDrive of each service email account and only 1 or 2 members of staff have password. This ensures that the majority of staff cannot access documents on non-Impact provided equipment. However Service Managers have the potential to access their OneDrive documents on non-Impact computers. • Use of confidential paper waste disposal service • Secure and alarmed buildings	**2**	**4**	**M**

Risk	Mitigation	L	S	Level
	• Detail of requirements regarding confidentiality in staff terms and conditions • Information including photograph permission forms used • Positioning of computer screens			
A person may change what information they have agreed can be shared and this is not shared to all concerned	• Information kept for a limited amount of time • People informed at beginning of service what info will be shared and option of and how to change permission • Posters regarding confidentiality and DTP in buildings where service users meet. • Regular checks with people regarding sharing of info throughout intensive work e.g. advocacy – 'you previously said I could share our conversations with your family are you happy for me to share today's conversation?'	**2**	**4**	**M**
New information sharing requests may be made by commissioners and are given without consent	• Through training and policies, staff understand this would need to be checked with a manager and or service users before being given • Through training and policy staff would understand this can be refused under GDPR legislation	**1**	**4**	**L**
Information collected needs to be changed e.g. new CCTV installed which does not conform with GDPR legislation	• Through training and policies staff know this would need to be checked prior to being used • The organisation has a data controller who understands or can get external advice prior to changes being made	**1**	**4**	**L**
Information shared with other orgs may be used inappropriately	• Checks will be made with partner organisations to establish that they understand GDPR legislation and are compliant • Information sharing will be a standard clause in partnership agreements and contracts	**1**	**4**	**L**

Risk	Mitigation	L	S	Level
	• Sharing information with other relevant organisations will be included on consent forms			
Identifiers may be collected which prevent anonymity	• Only information vital to providing the best service will be shared • Service users, staff and volunteers will be clear through consent forms/clauses what information will be shared so will be aware of the risk of this • Through training staff will understand they should get specific consent prior to sharing information e.g. 'Are you happy for me to share your health issue with your manager and/or colleagues? • Information will be given on the potential impact of sharing or not, so an informed decision can be made	**1**	**4**	**L**
Vulnerable people may withdraw from a service as they do not want to be identified	• Clear information which meets new legislation in a relevant and understandable format will be given so informed decisions can be made • Negotiation of limited information only, may be possible through discussion with a manager • A record will be made that this occurred so information required can be re-assessed and clarity for all concerned why requested info is needed	**1**	**4**	**L**
Information stored beyond agreed time limits eg time after service ceases which is against legislation	• A register of how long records need to be kept will be in place and accessible to all relevant staff • Retention of records included in the confidentiality and data protection policies • Secure arrangements are in place for disposal	**1**	**3**	**L**
Information collected is not securely stored	• Managers will have responsibility to ensure staff and volunteers now how information should be stored • Appropriate equipment will be supplied e.g. lockable filing cabinets, password-protected computers, encrypted backups	**1**	**4**	**L**

Risk	Mitigation	L	S	Level
Information is taken away from premises which could be lost or stolen	• A clear policy on how to store and transfer paper information in place and all sign to say understand and agree to implementation • Creation of limited need to take information in paper form from offices and secured IT devices provided • Suitable equipment provided for storage at home where required e.g. advocates	**1**	**4**	**L**
Identification of an individual to others who are a danger to them	• No information given over the phone unless to someone positively identified • Permission required to share information with others who are not in an agreed professional capacity • Where there is an identified danger relevant staff aware contact may be made • Addresses of premises where vulnerable people are likely to be promoted or not appropriately e.g. Stopover • Relevant staff and volunteer levels in place to oversee visitors or phone calls	**1**	**4**	**L**
Reputational damage if legislation not adhered to	• Relevant policies and procedures in place • Relevant information in staff terms and conditions • Staff training completed • Updates on legislation communicated through newsletter, team meetings and managers meetings	**1**	**3**	**L**
Large fines if legislation not adhered to	• Relevant policies and procedures in place • Relevant information in staff terms and conditions • Staff training completed • Updates on legislation communicated through newsletter, team meetings and managers meetings	**1**	**5**	**L**

Risk	Mitigation	L	S	Level
Compensation claims from individuals affected by a breach of data protection	• Relevant policies and procedures in place • Relevant information in staff terms and conditions • Staff training completed • Updates on legislation communicated through newsletter, team meetings and managers meetings	**1**	**3**	**L**
Contracts withdrawn and partnerships dissolved if a breach occurs	• Clear clauses in contracts and partnership arrangements • Understanding and agreement with partners on how information sharing will be conducted and used • Staff training so all understand implications of holding and sharing data	**1**	**4**	**L**