

We believe that Participatory Artists deserve the deepest, richest support and development

*We believe in you!*

**Data Protection and Confidentiality**

**Purpose:** To advise all Interwoven members of their legal and contractual roles and responsibilities with regard to Data Protection including information on the Data Protection Act 1998.

*This policy will be replaced on 25th May 2018*

|  |  |
| --- | --- |
| **Owner** | Director of Policy  |
| **Approved**  | 09/02/2018 |
| **Policy Number**  | CORP/003 |
| **Review Date**  | 09/04/2018 |
| **Change History** |
| **Version**  | **Date**  |  **Summary of Change**  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Policy Contents Page**

1. Introduction 3
2. Definitions 3
3. Roles & Responsibilities 4
4. The Eight Main Principles of the Data Protection Act 1998 5
5. Privacy Impact Assessment 8
6. Subject Access Requests 9
7. Incident Reporting 9
8. Misuse 10
9. Policy Review 10

**1 Introduction**

1.1 The **Data Protection Act 1998** (DPA) establishes a framework of rights and duties which are designed to safeguard personal data. The framework balances the legitimate needs for organisations to collect and use personal data for business and other purposes against the right of individuals to respect the privacy of their personal details.

1.2 As an organisation, we are bound by law to the fair and legal processing of ‘personal’ and ‘sensitive’ data of not only our customers/service users but also our employees, contractors and volunteers.

1.3 This policy applies to *all* Interwoven Board members, individual artists, contractors and volunteers with access to organisation and customer/service user data. Under the DPA *everyone* is legally responsible for the safeguarding of data.

1.4 In addition, the General Data Protection Regulation (GDPR) and Data Protection Bill will be the over-arching legal framework for all EU states from May 2018, giving the Information Commissioner’s Office who enforces Data Protection Act 1998 additional powers with regard to criminal prosecutions and monetary fines.

**2 Definitions**

2.1 ‘**Personal Data’** is defined under the DPA as “any information or combination of information that can be used to identify a *living* individual” for example,

* Address
* Date of Birth
* Passport number
* National Insurance Number
* Driving licence Number
* CCTV footage if the individual can be identified by the footage
* NHS Number

*Note:* A person’s name on its own is not enough information to identify an individual however when combined with other information such as an address, it then becomes “personal data” and is protected as such.

2.2 **‘Sensitive Data’** is defined under the DPA as information relating to any of the following with regards to a *living* individual,

* Ethnicity
* Gender
* Religious or other beliefs
* Political opinions
* Membership of a trade union
* Sexual orientation
* Physical or Mental Health Condition
* Offences committed or alleged to have been committed by that individual

2.3 In the collection of “**sensitive data**” the individual must “*opt-in*” and give explicit consent to the organisation collecting and holding this data type, you cannot automatically take it. In order to gain consent when collecting sensitive data, you must clearly explain the following;

* Why you want the data?
* How it will be used?
* How you will store it (security arrangements)?
* Who you will share it with?
* How long you will hold it for?

2.4 For the purposes of this organisation, the following two additional categories of data are also protected as “sensitive data” and they are;

* Any data relating to Children – *a child is legally defined as anyone under 19 years old under this Act.*
* Financial Data

2.5 **‘Data Owner’** is defined as the body or organisation providing data for contractual or business purposes.

2.6 ‘**Data Processor’** is defined as the body or organisation that processes data on behalf of the ‘Data Owner’ for contractual or business purposes. Once the contract term is complete the Data Processor is legally and contractually obliged to return the data held to the Data Owner.

2.7 **‘Data Subject’** is defined as any living individual who is the subject of personal data whether in a personal or business capacity

2.8 **‘Data’** is defined as information stored electronically i.e. on computer, including word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or databases, faxes and information recorded on telephone logging systems in addition to manual records which are structured, accessible and form part of a ‘relevant filing systems’ (filed by subject, reference, dividers or content), where individuals can be identified and personal data easily accessed without the need to trawl through a file.

**3 Roles and Responsibilities**

3.1 The Data Protection Officer has overall responsibility for all data processed and held within the organisation (both electronically and physically).

3.2 The Interwoven Board Member are responsible for ensuring all aspects of Data Protection Law is adhered to.

3.3 Interwoven members, individual artists, contractors and volunteers are responsible for adhering to this policy and ensuring any data they have access to is held securely and processed in line with the data subjects rights.

**4 The 8 Main Principles of the Data Protection Act 1998**

4.1 The DPA contains 8 main principles for good data handling and as an organisation we are legally bound to ensure we not only follow them but embed them within our operations and ethos. The 8 main principles direct that all personal and sensitive information must be;

1. ***fairly and lawfully processed*** - In practice, it means that you must:
* have legitimate grounds for collecting and using the personal data;
* not use the data in ways that have unjustified adverse effects on the individuals concerned;
* be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
* handle people’s personal data only in ways they would reasonably expect; and
* make sure you do not do anything unlawful with the data.
1. ***processed for limited purposes*** - In practice, the second data protection principle means that you must:
* be clear from the outset about why you are collecting personal data and what you intend to do with it;
* comply with the Act’s fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
* comply with what the Act says about notifying the Information Commissioner; and
* ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.
1. ***adequate, relevant and not excessive*** - In practice, it means you should ensure that:
* you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
* you do not hold more information than you need for that purpose.
1. ***accurate and up to date*** - To comply with these provisions you should:
* take reasonable steps to ensure the accuracy of any personal data you obtain;
* ensure that the source of any personal data is clear;
* carefully consider any challenges to the accuracy of information; and
* consider whether it is necessary to update the information.
1. ***not kept longer than necessary*** - In practice, it means that you will need to:
* review the length of time you keep personal data;
* consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
* securely delete information that is no longer needed for this purpose or these purposes; and
* update, archive or securely delete information if it goes out of date.
1. ***processed in line with the data subjects’ rights*** - and the rights of individuals that it refers to are:
* a right of access to a copy of the information comprised in their personal data;
* a right to object to processing that is likely to cause or is causing damage or distress;
* a right to prevent processing for direct marketing;
* a right to object to decisions being taken by automated means;
* a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
* a right to claim compensation for damages caused by a breach of the Act.
1. ***kept secure*** - In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:
* design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
* be clear about who in your organisation is responsible for ensuring information security;
* make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
* be ready to respond to any breach of security swiftly and effectively.
1. ***not transferred to other countries without adequate protection*** – In practice, it will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas and how the information is sent and the necessity to have contracts in place when using sub-contractors abroad.

4.2 The Quality & Compliance Manager can provide further advice and guidance on these principles and how they affect your role and the organisation.

**6** **Privacy Impact Assessment**

6.1 A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information.

6.2 Completion of a PIA is to be considered in the following circumstances:

* introduction of a new paper or electronic information system to collect and hold personal data;
* update or revision of a key system that might alter the way in which the organisation uses monitors and reports personal information.
* changes to an existing system where additional personal data will be collected proposal to collect personal data from a new source or for a new activity
* plans to outsource business processes involving storing and processing personal data
* plans to transfer services from one provider to another that include the transfer of information assets
* any change to or introduction of new data sharing agreements

This list is not exhaustive.

6.3 The completion of a PIA will become a legal requirement from 2017 as part of the General Data Protection Regulation (GDPR) and therefore they should be completed in all appropriate circumstances as part of “best practice” prior to the introduction of the new legal framework.

6.4 The Data Protection Officer will assist the Interwoven Board with the process of completing any required PIA using the organisational template.

**7 Subject Access Requests**

7.1 A Subject Access Request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998 (DPA).

7.2 This means any customer/service user or customer advocate, Interwoven member, individual artist, contractor or volunteer has the legal right to the information held about them by the organisation.

7.3 When an individual makes a written Subject Access Request, the organisation has **40 days** to respond with full disclosure. Should a member of staff receive such a request then they must pass the written request to the Data Protection Officer ***immediately***.

7.4 The Data Protection Officer can then co-ordinate the collection of the data and check the contents to ensure it does not contain any other individual’s data (and therefore breaches their rights) before responding to the SAR.

7.6 The Data Protection Officer will check the validity of each SAR to ensure the requester has the legal right to the information held by the organisation.

**8 Incident Reporting**

8.1 An incident involving data loss or corruption or breach including (*but not limited to*)

* Lost/missing/stolen paper files and/or single documents containing personal and/or sensitive data
* Corrupted or missing electronic data
* Unintentional data share (paper or electronic) with unauthorised person/organisation
* Someone has accessed data that they shouldn’t have
* A successful phishing scam (please refer to the phishing policy)
* Unauthorised copying of paper or electronic data
* Virus or successful hacking breach

8.2 All incidents should be reported ***immediately*** to the Data Protection Officer for further investigation.

8.4 The Data Protection Officer will ensure the correct legal notifications are made and any resulting actions are followed in liaison with the Interwoven Board

**9 Misuse**

9.2 Any individual who fails to adhere to these principles will subject themselves to disciplinary action, up to and including dismissal; in addition such unauthorised access is liable for prosecution as a criminal offence under Section 55 of the Data protection Act 1998 or an action for civil action under the same Act.

9.3 The Information Commissioner’s Office (ICO) who monitors and enforces adherence to the DPA can fine companies and individuals *up to £500,000* for breaches or misuse of the Act.

**10 Policy Review**

10.1 This policy will be reviewed annually unless there is a change of law, guidelines or contractual obligation and maybe subject to change.