Document 2018.1	**YIFM Data Protection Policy**
What is this?	Data Protection Policy Version 1.0
Governance Code Section:	Data Protection Policy (DPP)
Notes:	*GDPR Regulation Update*
	Final Version: Issue 24th May, 2018

YIFM Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Young Irish Filmmakers (YIFM). This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), the Irish Data Protection (Amendment) Act (2003) and the General Data Protection Regulation ("the GDPR") (Regulation (EU) 2016/679)

Rationale

YIFM as an organisation must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by YIFM in relation to its staff, service providers and clients in the course of its activities.

Scope

The policy covers both personal and sensitive personal data (Electronic & Non-Electronic) held in relation to Data Subjects by YIFM. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care by YIFM. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

Definition

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy:

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of YIFM.
Data Controller	YIFM
Data Subject	A living individual who is the subject of the Data, i.e. to whom the data relates either directly or indirectly.

Data Processor	A person or entity who processes Data on behalf of YIFM on the basis of a formal, written contract, but who is not an employee of YIFM, processing such Data in the course of his/her employment.
Data Protection Working Group	YIFM has established a Data Protection Working Group which will monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients. Any Data Protection enquiries should be directed to dpo@yifm.com
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

YIFM as a Data Controller

In the course of its daily organisational activities, YIFM acquires, processes and stores personal data in relation to:

- Employees of YIFM
- Members of YIFM
- Customers of YIFM
- Third party service providers engaged by YIFM
- Sponsors

In accordance with Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation.

However, YIFM is committed to ensuring that all staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Working Group is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by YIFM, there is a regular and active exchange of personal data between YIFM and its Data Subjects. In addition, YIFM exchanges personal data with Data Processors on the Data Subjects' behalf. This is consistent with YIFM's obligations under the terms of its contracts with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Working Group to seek clarification.

Subject "Access Requests"

Any formal/written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Working Group, and, if valid, will be processed as soon as possible, but within 30 calendar days. It is intended that by complying with these guidelines, YIFM will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party Processors

In the course of its role as Data Controller, YIFM engages a number of Data Processors to process Personal Data on its behalf.

In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation.

These Data Processors include:

- Third Party service providers engaged by YIFM

The Data Protection Principles:

The following key principles are enshrined in Irish legislation and are fundamental to YIFM's Data Protection policy.

In its capacity as Data Controller, YIFM ensures that all data shall:

1. Be obtained and processed fairly and lawfully.

For data to be obtained fairly, the Data Subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (YIFM)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

YIFM will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, YIFM will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- YIFM intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;

The Data Protection Principles (cont'd)

- Processing of the personal data will be carried out only as part of YIFM's lawful activities, and it will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to YIFM and operating on its behalf, or where YIFM is required to do so by law.

2. Be obtained only for one or more specified, legitimate purposes.

YIFM will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which YIFM holds their data, and it will be able to clearly state that purpose or purposes.

3. Not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by YIFM will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure.

YIFM will employ high standards of security in order to protect the personal data under its care.

Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation.

5. Be kept accurate, complete and up-to-date where necessary.

YIFM will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. YIFM conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.

YIFM will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

The Data Protection Principles (cont'd)

7. **Not be kept for longer than is necessary to satisfy the specified purpose(s).**

YIFM has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, YIFM undertakes to destroy, erase or otherwise put this data beyond use.

8. **Be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.**

YIFM has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, YIFM's staff engages in active and regular exchanges of information with Data Subjects. Where a valid, formal request is submitted by a Data Subject in relation to the data held by YIFM, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which YIFM must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

YIFM's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Working Group in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 30 calendar days from receipt of the request.

Implementation

As a Data Controller, YIFM ensures that any entity which processes Personal/organisational Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation through the Data Sharing Confidentiality Agreement. Regular audit trail monitoring will be done to check compliance with the Agreement by any third-party or entity which processes Personal/organisational Data on behalf of YIFM.

Failure of a staff member to manage YIFM's data in a compliant manner maybe viewed as a breach of contract, and lead to disciplinary action.

Failure of YIFM's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Appendix 1

YIFM

Subject Access Request Procedure

To see a copy of your own data held by YIFM, you will need to submit a written request to the Data Protection Working Group (dpo@yifm.com), enclosing proof of identity, such as copy of driving licence or passport. YIFM will respond as quickly as possible, but has a maximum of 30 calendar days to respond to your request once it has received all the relevant information.

The postal address for subject access requests is:

Data Protect Request,

Data Protection Working Group - YIFM,

St. Joseph's,

Waterford Road,

Kilkenny

The email address for subject access requests is:

dpo@yifm.com

Appendix 2

YIFM- Data Retention & Destruction Policy

The purpose of this Data Retention and Destruction Policy is to ensure that YIFM retains its official records in accordance with the requirements of all applicable Data Protection laws and to ensure that official records no longer needed by YIFM are discarded at the proper time.

The Document Retention and Destruction Policy defines YIFM's procedures for retaining and destroying documents containing Confidential or Restricted data types. This policy covers all records and documents, regardless of physical form (including electronic documents), and contains guidelines for how long certain documents should be kept and how records should be destroyed.

This Policy applies to all official records generated in the course of YIFM's operations, including but not limited to:

- typed, or printed hardcopy (i.e., paper) documents;
- electronic records and documents (e.g., email, Web files, text files, PDF files);
- video or digital images;
- graphic representations;
- records on storage devices;
- electronically stored information contained on network servers and/or document management systems; and
- recorded audio material (e.g., voicemail).

This document is intended to be read along with the Data Protection Policy.

All employees responsible for the retention of records are also responsible for the proper destruction of records following the stated retention period. Manual records must be destroyed by shredding or other means to ensure that all sensitive or confidential material can no longer be read or interpreted.

Administration

a. Record Retention Schedule. Attached to this Policy is a Record Retention Schedule (Attachment A) that is approved as the maintenance, retention and disposal schedule for official records of YIFM.

b. Authority and Responsibility of the DPWG The DPWG shall be authorized to: (a) review and make modifications to the Record Retention Schedule from time to time to ensure that this Policy complies Data Protection laws and includes the appropriate document and record categories for YIFM; (b) monitor the compliance of YIFM employees with this Policy; and (c) take such other action as may be authorized by YIFM's Board of Directors.

c. Distribution of Policy to Employees. The DPWG will arrange for every employee to receive a copy of this Policy and each such employee shall sign a statement (Attachment B) that affirms that he or she has received a copy of this Policy, has read and understands it, and has agreed to comply with it. There will be a training for staff as part of the roll-out of the Policy.

DOCUMENT DESTRUCTION PROCEDURES

Once records have been retained for the applicable period set forth in the Record Retention Schedule, they should be prepared for destruction in the manner prescribed by the DPWG, unless the DPWG in consultation with the board has suspended the destruction of any records for reasons of litigation or audit.

SUSPENSION OF RECORD DISPOSAL IN EVENT OF LITIGATION OR CLAIMS

In the event any employee of YIFM reasonably anticipates or becomes aware of an audit or the commencement of any litigation against or concerning YIFM, such employee shall inform the DPWG and any further disposal of documents shall be suspended until such time as the DPWG, with the advice of the CEO, determines otherwise. The DPWG shall take such steps as are necessary to promptly inform affected staff of any suspension in the disposal or destruction of documents.

All paper documents destroyed pursuant to this Policy shall be cross-cut by mechanical shredder by the DPWG. Electronic data contained on servers and hard drives shall be deleted and overwritten also by the DPWG. Electronic data contained on all other media shall be destroyed by the physical destruction of that media.

RECORD RETENTION SCHEDULE

This Record Retention Schedule sets forth an abbreviated schedule of key record-keeping holding periods and maintenance requirements. It is not intended to and does not provide a complete compilation of all records.

Type of Data / Record /	**Retention Period**
Membership record	5 Years
Financial record	7 Years
Tax record	7 Years
Income record	7 Years
Organisation data	2 Years
Individual data	5 Years
Staff record	5 Years
Board record	5 Years

If you have questions about the retention or destruction of specific documents or the data types they contain, please contact the Data Protection Working Group (dpo@yifm.com)

Appendix 3

YIFM - Data Retention Periods Policy

1.0 Introduction

Section 2 (1)©(iv) of the Data Protection Act says: "the data shall not be kept for longer than is necessary for that purpose or those purposes".

A wide variety of records are held by YIFM including membership records, online orders, financial records, HR records and general administrative records. An increasing number of records are stored electronically. This document outlines the minimum retention period for records held by YIFM and applies to records of all types regardless of the medium on which they are held. This policy guarantees that there is a specific responsibility by YIFM for ensuring that files are regularly purged and that personal information is not retained any longer than necessary.

2.0 Definition of Record

A record is defined under the Freedom of Information Acts 1997 and 2003 as "any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (within the meaning of the Data Protection Act, 1988 and 2003) are held, any other form (including machine-readable form) or device in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form of any of the foregoing or is a combination of two or more of the foregoing" (Freedom of Information Act, 1997, 2003).

Records created by YIFM should be both accurate and complete. They must provide evidence of the function or activity they were created to document. In order to be evidential, records must be authentic, reliable, have integrity and be usable.

2.1 **An authentic record** is one that can be proven to be what it purports to be. In order to ensure that the records created are authentic then records should be dated, timed and signed. They should be placed into the filing system to form part of the retention schedule so that they are protected against unauthorised addition, deletion or alteration.

2.2 **A reliable record** is one that can be trusted to be an accurate representation of a function. Therefore, records should contain all relevant facts and be created at the time of the action or transaction or as soon as possible afterwards by a person authorised to carry out that function, action or transaction.

2.3 **The integrity** of a record refers to it being complete and unaltered. Once created, additions or annotations to the record can only be carried out by those authorised to do so and any amendment should be explicitly indicated on the record.

2.4 **A useable record** is one that can be located, retrieved, presented and interpreted or read whenever or wherever there is a justified need for that information. It should be traceable within a records management system. Record

schedules and filing indices that capture the records are essential in ensuring records are useable.

In electronic records, contextual information is required in addition to the physical transfer of records to ensure their continued usability.

2.5 Records retained should be original (or an electronic copy, transferred using the appropriate and verifiable system), unique or of continuing importance to YIFM.

3.0 Record Retention Periods

Legal obligation and good practice

YIFM must comply with the provisions of section 2(1)(c) of the Data Protection Acts 1988 and 2003 and the General Data Protection Regulation ("the GDPR") (Regulation (EU) 2016/679)

The Acts set out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained.

This requirement places a responsibility on YIFM to be clear about the length of time personal data will be kept and the reasons why the information is being retained.

This policy is in compliance with those provisions and includes defined retention periods for records and systematic disposal of records within a reasonable period after the retention period expires.

Type of Record	**Retention Period**
Membership	5 Years
Financial	7 Years
Online Orders	7 Years
Employee	5 Years
Tax	7 Years
Suppliers	7 Years

Appendix 4

YIFM - Record Retention and Destruction Affirmation for Staff Members

AFFIRMATION STATEMENT

I, _____, have read and understand the foregoing Record Retention and Destruction Policy of YIFM and hereby agree to comply with same.

_____

Name of Employee

_____

Title

_____

Date

Appendix 5

YIFM - Data Loss Notification Procedure

Introduction:

The purpose of this document is to provide a concise procedure to be followed in the event that YIFM becomes aware of a loss of personal data held by it. This includes obligations under law, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003) and the General Data Protection Regulation ("the GDPR") (Regulation (EU) 2016/679).

It is also in line with the Data Breach Notification Obligation in 2011 legislation.

Rationale:

The response to any breach of personal data (as defined by the legislation) can have a serious impact on YIFM's reputation and the extent to which the public perceives YIFM as trustworthy.

The consequential impact on the commercial brand can be immeasurable. Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification.

This guide is to assist YIFM staff in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Scope:

The policy covers both personal and sensitive personal data held by YIFM. The policy applies equally to personal data held in manual and automated form. All Personal Data will be treated with equal care by YIFM.

This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request procedure, the Data Retention and Destruction Policy and the Data Retention Periods List.

What constitutes a breach, potential or actual?

A breach is any unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form.

This could mean:

- Loss of a laptop, storage device or mobile device that contains personal data
- Emailing records in error or emailing multiple recipients and revealing their email addresses.
- Giving a system login to an unauthorised person
- Failure of a door lock to a server room or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to YIFM's Data Protection Working Group.

Any employee who becomes aware of a likely data breach and fails to notify the DPO will be subject to YIFM's disciplinary procedure.

A team comprising of a member of the DPWG and other relevant staff will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances YIFM may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. YIFM will make recommendations to the data subjects which may minimise the risks to them. YIFM will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner. The only exceptions to this policy are when the data subjects have already been informed, and where the loss involves only non-sensitive, non-financial personal data.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

Data Loss Incident logging.

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request.