



## Data Protection Policy

MetFilm School and MetFilm Ltd

Owner:	Chris Maples
Approving Body:	Executive Team
Date of Approval:	May 2018
Version:	2.3

Queries relating to this document should be referred to:  
Chris Maples  
Email: [chrism@metfilm.co.uk](mailto:chrism@metfilm.co.uk)

## Table of Contents

1.	General principles.....	3
2.	Definitions.....	3
3.	What is Data Protection Legislation?.....	5
4.	Data protection principles.....	6
5.	Legal basis for processing.....	7
6.	Other responsibilities under Data Protection Legislation .....	9
7.	Notification .....	10
8.	Collection and Processing of Data.....	10
9.	Data Storage, Retention and Disposal .....	12
10.	Data Security .....	13
11.	Staff Duties .....	14
12.	Security Procedures .....	14
13.	Disclosure .....	15
14.	Confirmation of Student Status .....	15
15.	Disclosing data to a third party .....	15
16.	Disclosing personal data overseas .....	15
17.	Exemptions.....	16
18.	Rights of Access .....	16
19.	Breach of the Policy .....	20
20.	Appendix .....	21
	Appendix A Notified Purposes .....	21
	Appendix B Collection Guidelines .....	23
	Appendix C Disclosure Guidelines .....	24
	Appendix D Using Personal Data for Direct Marketing.....	31
	Appendix E Reference Guidelines .....	32
	Appendix F Examinations and Assessments .....	34
	Appendix G Telephone Guidance .....	35
	Appendix H Funding Body Purposes.....	37

## 1. General principles

- 1.1. MetFilm is committed to the protection of individuals' rights and privacy. This Policy has been developed to provide detailed guidance on the correct and lawful processing of personal data, to ensure that all staff, students and other workers who process personal data on behalf of MetFilm are doing so in accordance with all UK Data Protection Legislation.
- 1.2. The Policy applies to all staff, students, suppliers, and others with whom MetFilm has dealings.
- 1.3. A breach of the Data Protection Policy by members of staff or students will be considered as a disciplinary offence and will be dealt with in accordance with MetFilm's disciplinary procedures. In addition, a breach of the Policy may expose MetFilm and individual concerned to criminal or civil liabilities. In addition to any business liability, staff may also personally liable. Data subjects may also apply to court for compensation if they have suffered damage from such a loss.
- 1.4. MetFilm needs to process certain personal information about its staff (for example relating to recruitment and salary) and students (relating to the administration of courses of study, to record progress, to agree awards, to collect fees) in order to fulfil its purpose and to meet its legal obligations to funding bodies and the government.
- 1.5. The processing of personal information such as the collection, recording, use, and storage of personal information must be dealt with lawfully and correctly in accordance with all relevant UK regulations. All information containing personal data must be protected against unauthorised access, accidental loss or destruction, modification or disclosure.
- 1.6. MetFilm regards the lawful and correct treatment of personal information as important to its successful operation, and to maintain confidence between those with whom we deal and ourselves.

## 2. Definitions

- 2.1. Personal Data
  - 2.1.1. "Personal Data" means data relating to a living individual who can be identified: from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.
  - 2.1.2. Personal data can be either factual (such as name, address, telephone, images and photographs) or an expression of opinion about the individual

(such as a performance appraisal or comments on scripts) including any intentions of the data controller or any other person in respect of that individual.

2.1.3. Personal data covers any information which relates to an individual in any format (written or oral). Examples include:

2.1.3.1. a student or staff file

2.1.3.2. an email about someone

2.1.3.3. a post-it note with someone's name and telephone number

2.1.3.4. Information provided orally about the student's personal circumstances.

2.2. Special Category Data

2.2.1. "Special Category Data" consists of personal data relating to:

2.2.1.1. ethnic origin,

2.2.1.2. physical and mental health (including, for example, details of the reasons for an individual's sick leave),

2.2.1.3. sex life,

2.2.1.4. religion or belief,

2.2.1.5. political opinion

2.2.1.6. information relating to alleged or actual criminal offences

2.2.1.7. Trade Union membership

2.2.1.8. The more 'sensitive' the nature of the data the more securely it should be treated in terms of deciding whether it is necessary to obtain it, the method of obtaining it, whether to retain/disclose it and how to retain/disclose it.

2.3. Processing

2.3.1. "Processing" means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

2.4. Data Subject

2.4.1. "Data subject" means an individual who is the subject of the personal data.

2.5. Data Controller

- 2.5.1. “Data controller” means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any personal data is processed. In this case, this means MetFilm or nominated individuals acting on behalf of and with the authority of MetFilm.
- 2.6. Data Processor
  - 2.6.1. “Data Processor” means any person (other than a member of staff) who processes data on behalf of MetFilm.
- 2.7. Information Commissioner
  - 2.7.1. The UK’s independent body set up to uphold information rights
- 2.8. Staff
  - 2.8.1. Unless otherwise applicable, all references to staff include all current, past and prospective staff, full time, part time staff and Members of the Board of Governors as well as agency workers, temporary workers and contractors.
- 2.9. Students
  - 2.9.1. Unless otherwise applicable, all references to students include all current, past and prospective students, whether full-time or part-time.

### 3. What is Data Protection Legislation?

- 3.1. Data Protection Legislation sets out rules and standards for the use and handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects') by organisations ('data controllers').
- 3.2. The law applies to organisations in all sectors, both public and private. It applies to all electronic records as well as many paper records. It doesn't apply to anonymous information or to information about the deceased.
- 3.3. Until 24 May 2018, the legislation in the UK is the Data Protection Act 1998 (DPA 1998). From 25 May 2018, this will be superseded by the EU General Data Protection Regulation (GDPR), coupled with a new Data Protection Act that supplements the GDPR in specific ways. All of the legislation is based around the notions of principles, rights and accountability obligations. The legislation is regulated in the UK by the Information Commissioner's Office (ICO) as well as the courts.
- 3.4. Under the DPA 1998, MetFilm School Ltd and MetFilm School maintains data protection registrations (also known as a notification) with the ICO. This outlines, in

very general terms, the personal data being processed by the respective companies.

- 3.5. The Act applies to any information about a living individual (e.g. students, staff members, etc.). Essentially, staff handling any information about people as part of their job will need to comply with Data Protection Legislation.
- 3.6. Our Data Protection Officer can be contacted at any time by emailing [data@metfilm.co.uk](mailto:data@metfilm.co.uk)

## 4. Data protection principles

- 4.1. Data Protection Legislation requires that personal data shall be:
  - 4.1.1. processed lawfully, fairly and in a transparent manner in relation to individuals;
  - 4.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
  - 4.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - 4.1.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
  - 4.1.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
  - 4.1.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”
- 4.2. And requires that
  - 4.2.1. the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

## 5. Legal basis for processing

- 5.1. We must have a valid lawful basis in order to process personal data.
- 5.2. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose of data processing or collection and the relationship with the individual.
- 5.3. Most lawful bases require that processing is 'necessary'. If we can reasonably achieve the same purpose without the processing, we won't have a lawful basis.
- 5.4. We must determine our lawful basis before we begin processing, and we should document it. We should take care to get it right first time and we should not swap to a different lawful basis at a later date without good reason.
- 5.5. Our privacy notice should include our lawful basis for processing as well as the purposes of the processing.
- 5.6. If our purposes change, we may be able to continue processing under the original lawful basis if our new purpose is compatible with our initial purpose (unless our original lawful basis was consent)
- 5.7. If we are processing Special Category Data we need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- 5.8. If we are processing criminal conviction data or data about offences we need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- 5.9. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:
  - 5.9.1. Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
  - 5.9.2. Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
  - 5.9.3. Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
  - 5.9.4. Vital interests: the processing is necessary to protect someone's life.
  - 5.9.5. Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in

law.

5.9.6. Legitimate interests: the processing is necessary for our 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.

5.10. Special Category Data - When processing special category data, one of the following conditions must also apply. These are listed in Article 9(2) of the GDPR:

5.10.1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

5.10.2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

5.10.3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

5.10.4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

5.10.5. processing relates to personal data which are manifestly made public by the data subject;

5.10.6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

5.10.7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

5.10.8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the

management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

- 5.10.9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- 5.10.10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

## 6. Other responsibilities under Data Protection Legislation

### 6.1. The School

- 6.1.1. MetFilm Ltd and MetFilm School Ltd as corporate bodies are the data controllers and are committed to the protection of rights and privacy of individuals (includes students, staff and others) in the processing of personal data.
- 6.1.2. The Directors and all those in managerial or supervisory roles are responsible for developing and maintaining good information handling practice within MetFilm in accordance with this Policy and the Information Security Policy. They are also responsible for ensuring that all staff are trained in Data Protection and are aware of their responsibilities.

### 6.2. Staff

- 6.2.1. All staff or others who process or use any personal data must ensure that they follow the data protection principles and the guidance provided in the Data Protection Policy at all times.
- 6.2.2. All staff must report any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data directly to a Director.

### 6.3. Staff/Students as Data Subjects

- 6.3.1. All staff and students are responsible for:

6.3.1.1. Checking that any information that they provide to MetFilm is both accurate and up to date;

6.3.1.2. Informing MetFilm of any changes to information which they have provided, i.e. changes in addresses; and

6.3.1.3. Informing MetFilm of any errors in the information it holds about them.

#### 6.4. Data Protection Training

6.4.1. All staff should undertake regular Data Protection Training. Data Protection training and data protection seminars will be held to assist members of staff with an understanding of their legal duty under the Act. Staff in key roles will be provided with additional Data Protection training.

6.4.2. Data Protection training will be a part of a new member of staff's induction.

6.4.3. Failure to complete any Data Protection training may give rise to disciplinary action.

## 7. Notification

7.1. As a Data Controller, MetFilm Ltd and MetFilm School Ltd is required to notify the Information Commissioner's Office of the purposes for which it processes personal data. The list of purposes for processing personal data can be found at Appendix A Notified Purposes. MetFilm's notification is also published on the Information Commissioner's website at <https://ico.org.uk>. Anyone who intends to process personal data for purposes not included in MetFilm's Notification should seek authorisation and advice from a Director.

## 8. Collection and Processing of Data

8.1. Whenever personal data is collected, members of staff should make clear to the data subject what purpose(s) the information is be used for and, where necessary, obtain consent to the processing of the data. In most instances consent to process personal data is obtained routinely by MetFilm (e.g. when a student signs a registration form or when a new member of staff signs a contract of employment). For sensitive data, explicit written consent must always be obtained from the data subject.

8.2. Any School forms (whether paper-based or web-based) that gather data on an individual should contain a fair processing notice which explains the following:

- 8.2.1. Why the data is being gathered and how the data will be used;
  - 8.2.2. To whom the data may be disclosed to within MetFilm and to any outside third parties;
  - 8.2.3. The fact that completion of the form will be taken as consent given to the use of the data as outlined.
- 8.3. Samples of the suggested wording to adopt are provided in Appendix B.
- 8.4. Apart from Marketing, Education, Admissions, Finance and Registry teams, no other Departments should routinely be collecting and storing student's personal data except for one off instances such as field trips for health, safety purposes and attendance monitoring. Where consent is not provided for certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.
- 8.5. Data Collection Forms
- 8.5.1. Data collection forms must be approved by a Director before they can be used.
  - 8.5.2. Where a form is set up digitally it should always include a 'hidden' field value that identifies the legal basis on which the data is being collected.
  - 8.5.3. Each form should have a Legal Basis for Data Collection form completed which documents the legal basis for the data collection occurring.
- 8.6. Adequate, relevant and not excessive
- 8.6.1. The Legislation only permits the collection of adequate, relevant and not excessive amount of personal data. This means that only the personal data required for the specific purpose(s) notified to the data subject should be collected. Any data which is not necessary for that purpose(s) should not be collected.
- 8.7. Processing for limited purposes
- 8.7.1. Staff may only process data for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by Legislation and notified to the Information Commission's Office. This means that personal data must not be collected for one purpose and then used for another purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.
  - 8.7.2. All staff must take care to use personal data held by the School only for the purposes for which they were primarily intended, e.g.
    - 8.7.2.1. Staff, agent, and contractor administration;

- 8.7.2.2. Advertising, marketing, public relations, and general advice service;
  - 8.7.2.3. Accounts and records;
  - 8.7.2.4. Education;
  - 8.7.2.5. Student and staff support services;
  - 8.7.2.6. Research;
  - 8.7.2.7. Crime prevention and prosecution of offenders;
  - 8.7.2.8. Provision of commercial services;
  - 8.7.2.9. Publication of MetFilm magazine.
- 8.8. A more complete description of these purposes can be found in Appendix A Notified Purposes.

## 9. Data Storage, Retention and Disposal

- 9.1. It is the responsibility of the relevant senior manager to ensure that centralised records are maintained to meet the needs and reasonable expectations of students, MetFilm, and external bodies. For members of staff, the HR team within Finance has the responsibility of ensuring that centralised records are maintained.
- 9.2. Where possible central databases (such as Salesforce or Tribal EBS) should be used to avoid duplication of information and to increase data security. All local databases maintained by staff in the course of their duties containing personal data (including those using reference numbers for individuals rather than names) must be adequately secure (see Section 10).
- 9.3. MetFilm is required to ensure that all data is accurate and up-to-date. Staff and students have a responsibility to regularly update their records by contacting the administration team.
- 9.4. MetFilm should not retain personal data for longer than is necessary. This means that personal data should be destroyed or deleted when it is no longer required.
- 9.5. Members of staff should ensure that no personal data of prospective students, is kept longer than 7 years.
- 9.6. Members of staff should ensure that personal data of students and former students is retained no longer than 7 years if they have expressed a desire to stop being a part of our alumni community, unless it is determined to be necessary to meet our regulatory obligations.

- 9.7. Each Manager should ensure that their staff should regularly review their records to ensure that the documents they hold are destroyed within the relevant destruction time limit and in accordance with the relevant teams retention schedules.
- 9.8. Where the documentation contains personal information, the destruction must take place confidentially (e.g. shredding, disposal as confidential waste, secure electronic deletion).

## 10. Data Security

- 10.1. Each individual must ensure that personal data is processed in accordance with a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. This may mean avoiding use of email in favour of confidential post, the use of passwords or encryption for electronic documents and keeping papers under lock and key
- 10.2. The need for security is greater where sensitive personal data is involved. Particular care should be taken when staff are taking personal data off-site from their usual place of work as there is a greater risk of loss, theft or damage to personal data off-site. The transport of personal data in any format (laptop, hard copy, memory stick etc.) should therefore be avoided as far as possible. This applies especially to sensitive personal data, large volumes of personal data, or information which could cause particular harm or distress if lost. Only in exceptional circumstances should sensitive information be transported outside of the MetFilm premises. Staff who do so should always ensure that it is kept with them at all times. Staff should:
  - 10.2.1. Where possible use MetFilm Macs at campuses to access information as an alternative to transporting data.
  - 10.2.2. Only carry the minimum amount of personal data (e.g. avoid carrying the whole file if only one document is needed).
  - 10.2.3. It is MetFilm's intention that all mobile devices (laptops, smartphones, tablets) and external storage media (USB sticks, external hard drives, DVDs, CDs, etc.) used to transport personal data and sensitive personal data outside MetFilm will be secured by deploying strong encryption. Their loss/theft must be immediately reported to a Director and the Head of IT Operations.
  - 10.2.4. When working from home staff should:
  - 10.2.5. Use secure remote access facilities (VPN) instead of carrying work home;
  - 10.2.6. Never save documents containing personal data to a personal PC.

## 11. Staff Duties

- 11.1. All staff are responsible for ensuring personal data are kept securely and accessible only to those who need to use it. Appropriate security measures are to be taken to prevent accidental loss of, or damage to, personal data.
- 11.2. All staff and students are to ensure that they comply with the requirements set out in the Information Security and Email Usage policies. These policies are MetFilm's response to the legal obligation under legislation to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. They provide guidance on the usage and security procedure to follow when using MetFilm's IT systems.
- 11.3. Staff and others are to ensure that they comply with the security procedure set out below

## 12. Security Procedures

- 12.1. Electronic Records
  - 12.1.1. Care should be taken to ensure that PCs and terminals are not visible to unauthorised persons and that computer passwords are kept confidential.
  - 12.1.2. PC screens should not be left unattended without password protected screen-savers.
  - 12.1.3. Personal data should be password protected.
  - 12.1.4. Personal data should be encrypted when sent via email.
  - 12.1.5. Only encrypted memory sticks should be used to transfer personal data.
- 12.2. Manual Records
  - 12.2.1. Manual records should not be left where they can be accessed by unauthorised personnel.
  - 12.2.2. Personal data should be kept in a lockable room with controlled access, or in a locked drawer or filing cabinet.
- 12.2.3. Manual records should be shredded or disposed of through a confidential waste company.

## 13. Disclosure

- 13.1. Staff must not disclose personal data to a third party except in limited cases where there is a legal or statutory duty to do so. All staff must therefore take care to ensure that personal data is not disclosed to unauthorised third parties which includes family members of the data subject, friends, government bodies and the Police in certain circumstances without the data subject's consent.

## 14. Confirmation of Student Status

- 14.1. Student status is regarded as personal data under Data Protection Legislation. Confirmation of whether or not an individual is a student of MetFilm is therefore considered to be unauthorised disclosure of personal data.

## 15. Disclosing data to a third party

- 15.1. Personal data may only be transferred to a third-party processors if they agree to comply with those procedures and policies, or have in place adequate measures to do so.

## 16. Disclosing personal data overseas

- 16.1. You may not transfer personal data to countries outside of the European Economic Area (EEA) (the European Union Member States along with Iceland, Liechtenstein and Norway) unless the country or territory has an adequate level of protection for personal data.
- 16.2. Notwithstanding the above, there are however a number of non-EEA countries recognised by the European Commission to have adequate level of personal data protection ("approved countries"). Transfer of information to these countries will not breach the Data Protection Principles. The same applies to countries which have adopted the 'Safe Harbour'<sup>1</sup> Agreement (a set of rules similar to those found in the UK's data protection law) or the European Commission's model contractual clauses.
- 16.3. Information on the European Commission's list of approved countries, the 'Safe Harbour' agreement and the European Commission's model contractual clauses may be found on the Information Commissioners website (<https://ico.org.uk/>).
- 16.4. For non-EEA countries ensure that you check the European Commission's website to obtain the most up-to-date approved list of non-EEA countries and the status of

'Safe Harbour' agreement.

## 17. Exemptions

- 17.1. There are also exemptions which enable the transfer of personal data outside of the EEA even if there is no adequate protection. The most likely exemptions applicable to MetFilm are where:
  - 17.1.1. The data subject has given explicit consent
  - 17.1.2. The transfer is required for the performance of a contract
  - 17.1.3. The transfer is necessary for legal proceedings
- 17.2. No employees of MetFilm are authorised to transfer personal data outside of the EEA in these circumstances without the express, written approval of a Director.

## 18. Rights of Access

- 18.1. Subject Access Request
  - 18.1.1. Staff, students and other data subjects about whom MetFilm holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form.
  - 18.1.2. Any person wishing to exercise their right of access formally should complete a "Data Subject Access Form" and submit it along with evidence of proof of identity to prevent unlawful disclosure of personal data to a Director or the Registry team. (see Appendix I).
  - 18.1.3. An electronic copy of the Data Subject Access Form can be obtained from MetFilm's website.
  - 18.1.4. In normal circumstances, no charge will be made for a Subject Access Request. Please see our Subject Access Request Policy for full details.
  - 18.1.5. By law, MetFilm has one month from receipt of the request, fee and proof of identity, in which to respond to subject access requests, in any event MetFilm will endeavour to respond as quickly as possible. In limited circumstances, MetFilm may not be able to release personal data because exemptions under Legislation are applicable, or the disclosure of the data would release personal data relating to other individuals.

18.1.6. Students who wish to access copies of their student files or any other personal data should make a subject access request.

## 18.2. Email Access

18.2.1. The majority of e-mail communications that staff send or receive will be simple transactions regarding School business. Staff should avoid using e-mail to send personal information of a sensitive nature or to express views about individuals. This is because e-mail is an insecure medium and the sender has no control over the storage or use of the message after it has been sent.

18.2.2. Staff who receive by e-mail, from students or others, information that might be personal data or sensitive personal data should not retain such messages. They should print it out and delete the e-mail from their computer. (Examples might include any mention of individuals in relation to discipline or performance, family or personal circumstances.) The printed information should then be kept in the appropriate hard copy filing system in accordance with this Policy and be used strictly in accordance with this Policy.

18.2.3. MetFilm reserves the right to monitor the use of its e-mail facilities in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

## 18.3. Email Requests for Disclosure of Personal Data

18.3.1. Where possible requests for personal data by third parties should be made in writing on headed paper as a means of verifying that the request is genuine.

18.3.2. Email requests can be accepted on a case by case basis as long as you are satisfied the request is genuine. To verify whether a request is genuine, you need to:

18.3.2.1. Check the email is a valid address and that it is from an official email account;

18.3.2.2. Call the telephone number displayed on the email request to confirm the identity of the person requesting the personal data and that they are from the organisation they claim to be representing.

18.3.2.3. Once you are satisfied the request is genuine, you may respond by email to the request for personal information.

## 18.4. CCTV and Video Surveillance

18.4.1. MetFilm operates an IP based video surveillance system across its campuses and buildings, for the security and safety of its staff and students. Our cameras run on an isolated IP network with a proprietary Digital Video Recorder (DVR) system

- 18.4.2. MetFilm ensures the collection and retention of personal data obtained through the use of this footage complies with Data Protection Legislation.
- 18.4.3. MetFilm is committed to the protection and security of personal data especially as applied in the use, operation and monitoring of video surveillance images. As such:
  - 18.4.3.1. All security staff involved in the recording, observation and capture of images must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation.
  - 18.4.3.2. Only authorised persons involved in the monitoring or investigation can view video surveillance images.
  - 18.4.3.3. All recorded material will be treated as confidential and unless required for evidence will only be kept in accordance with policy guidelines.
  - 18.4.3.4. CCTV will not be retained for longer than necessary in accordance with the data protection principles.
  - 18.4.3.5. Data is stored and managed automatically by digital recorders which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a maximum of 1 month rotation in data retention.
  - 18.4.3.6. If video surveillance images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled and are to be erased when no longer required.

## 18.5. Direct Marketing

- 18.5.1. The Head of Marketing has responsibility for all outgoing mail or telephone marketing and for MetFilm's website. No personal data must be used or published in these contexts without the specific approval of a Director, including for alumni purposes.
- 18.5.2. Any department or services that use personal data for direct marketing purposes must inform the data subject of this at the time of collection of the information. Data subject must be provided with the opportunity to object to the use of their data for direct marketing purposes with an opt-out option on the form for example.
- 18.5.3. For further guidance see Appendix D Using Personal Data for Direct Marketing.

## 18.6. Research

- 18.6.1. Where personal data is collected ONLY for research purposes it is exempt from certain aspects of Data Protection Legislation

- 18.6.2. However, personal data collected for research purposes must not be used in forming any decisions about a particular individual, and must not be used in any way that will, or is likely to, cause distress to any data subject.
- 18.6.3. If you are collecting personal data for research within these parameters the following exemptions apply:
  - 18.6.3.1. Processing the personal data for additional research purposes (within the above parameters) other than those notified to the data subject on collection is permitted.
  - 18.6.3.2. Personal data processed only for research purposes (within the parameters) may be kept indefinitely.
  - 18.6.3.3. Personal data processed only for research purposes (within the parameters) and which is not made available in any form that identifies data subjects is exempt from the data subject's right of access.
- 18.6.4. Therefore, it is recommended that when personal data is collected for research purposes:
  - 18.6.4.1. The data subject should be informed of the purposes for which the data is being collected.
  - 18.6.4.2. Any data collection forms should make clear that the data will be used only for research, what the research is for, and that any published results will be anonymised.
  - 18.6.4.3. All other provisions of Data Protection Legislation apply, notably the requirement for adequate security when processing personal data whether or not within the above parameters.
- 18.6.5. Sensitive personal data
  - 18.6.5.1. The Data Protection (Processing of Sensitive Personal Data) Order 2000 allows the processing of sensitive personal data for research purposes where the following conditions are met:
    - 18.6.5.1.1. Data is not used to support measures or decisions about individuals without their explicit consent;
    - 18.6.5.1.2. The processing for research does not cause substantial damage or distress to any person;
    - 18.6.5.1.3. The processing for research purposes is in the substantial public interest.

## 18.7. References

### 18.7.1. References Provided by MetFilm

18.7.1.1. As part of its commitment to fair processing and openness MetFilm will disclose references provided by MetFilm to staff upon request. To obtain a copy of the reference a subject access request should be made in accordance with the procedure detailed within this Policy.

18.7.1.2. Staff are reminded that any reference they provide will be potentially disclosable to the individual by MetFilm or by the receiving third party. They must exercise due care and skill in providing a reference and ensure the reference is factually correct. Any expression of opinion should be reasonable and must be justified.

### 18.7.2. References Received by MetFilm

18.7.2.1. References received by MetFilm are not exempt from the right of access, this means that any references received by MetFilm will be disclosable. Referees from a third party should be informed that MetFilm's policy is to disclose references in a subject access request. Where the third party has expressed their refusal to give permission for disclosure of the information referees' personal details should be redacted and any other information which could identify them.

18.7.2.2. Further guidance on references can be found in Appendix E

## 19. Breach of the Policy

- 19.1. Should staff not process data in accordance with this Policy, MetFilm and the individual in breach could be liable to criminal prosecution and civil claims for damages.
- 19.2. If any member of staff or student is found to have breached this Policy, it will be considered to be a disciplinary offence. The individual may be suspended from having access to any personal data held by MetFilm and will be subject to action under MetFilm's Disciplinary Procedure.
- 19.3. If any staff member or student believes MetFilm has infringed her/his rights under this Policy, s/he should raise this concern under MetFilm's Grievance or Complaints Procedure respectively.
- 19.4. Any member of staff or student who considers that the Data Protection Policy is not being followed should raise the matter with their Head of Department in the first instance.

## 20. Appendix

### Appendix A Notified Purposes

MetFilm Ltd is registered as company number 04790426 and as a data controller with the Information Commissioners Office, our registration number is Z1335592 and you can find our registration here: <https://ico.org.uk/ESDWebPages/Entry/Z1335592>.

MetFilm School Ltd is registered as company number 06723644 as a data controller with the Information Commissioners Office, our registration number is Z228019X and you can find our registration here: <https://ico.org.uk/ESDWebPages/Entry/Z228019X>.

Our entry to the ICO for both companies can be found below:

1. Nature of work - Private School
2. Description of processing
  - The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.
3. Reasons/purposes for processing information
  - We process personal information to enable us to provide education and training conducted outside the State system, welfare and educational support services, to administer school property and library services, to maintain our own accounts and records, for administration in connection with boarding and the organisation of alumni associations and events, for fundraising purposes and to support and manage our staff. Our processing also includes the use of CCTV to maintain the security of the premises and for preventing and investigating crime.
4. Type/classes of information processed
  - We process information relevant to the above reasons/purposes. This may include:
    - i. personal details
    - ii. family details
    - iii. lifestyle and social circumstances
    - iv. financial details

- v. education and employment details
  - vi. disciplinary and attendance records
  - vii. vetting checks
  - viii. visual images, personal appearance and behaviour
  - ix. details of goods and services provided
- We also process sensitive classes of information that may include:
    - i. physical or mental health details
    - ii. sexual life
    - iii. racial or ethnic origin
    - iv. religious or other beliefs
    - v. trade union membership
    - vi. information relating to offences or alleged offences

#### 5. Who the information is processed about

- We process personal information about:
  - i. employees
  - ii. pupils and students
  - iii. professional advisers and consultants
  - iv. governors and members of school boards
  - v. sponsors and supporters
  - vi. services providers and suppliers
  - vii. complainants, enquirers
  - viii. individuals captured by CCTV images

#### 6. Who the information may be shared with

- We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of Data Protection Legislation. What

follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

- Where necessary or required we share information with:
  - i. educators, careers and examining bodies
  - ii. staff, students, governors and school boards
  - iii. current, past and prospective employers
  - iv. family, associates and representatives of the person whose personal data we are processing
  - v. central and local government
  - vi. healthcare professionals, social and welfare organisations
  - vii. police, courts, tribunals and security organisations
  - viii. voluntary and charitable bodies
  - ix. the media
  - x. financial organisations
  - xi. suppliers
  - xii. service providers
  - xiii. professional advisers

## 7. Transfers

- It may sometimes be necessary to transfer personal information overseas. When this is needed, information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

## Appendix B Collection Guidelines

1. MetFilm is fully committed to upholding the principles laid out in the Data Protection Act 1998 and the GDPR. MetFilm's Data Protection policy is available from MetFilm's website.
2. Data collection forms must be clearly titled to indicate their purpose(s) and collect only data relevant to those specific purpose(s). The legal basis must be identified prior to

data collection commencing, and the legal basis recorded on a 'Legal Basis for Data Collection' Form and stored in our SharePoint environment. All forms should include copy prior to the submission of data that sets out:

- 2.1 Who is collected the data
- 2.2 What the purpose of the data collection is for
- 2.3 How the data provided will be used by us
3. In addition, if any of the data may be transferred or used in ways that are not immediately obvious this must also be explained. Where any forms collect sensitive data (other than ethnic origin or disability information used solely for equal opportunities monitoring) the data subject's explicit consent to processing must also be obtained.
4. For this consent to be valid, the data subject must be aware of the purpose(s) behind the processing.
5. A Director must approve all data collection forms before they are used. Where small variations are made to forms, this approval is not necessary.

## Appendix C Disclosure Guidelines

### 1. Background

- 1.1. This section provides guidance on the main types of requests for student information and how to respond to them.
- 1.2. The students' handbook and enrolment form sets out the basis upon which MetFilm is collecting and disclosing student data and this should be referred to in the first instance.
- 1.3. The important thing to remember when dealing with requests for student information is that you cannot normally disclose anything without the student's consent, unless:
  - 1.3.1. There is a legal obligation to disclose,
  - 1.3.2. The disclosure is covered by an exemption under Data Protection Legislation,
  - 1.3.3. It is a serious emergency (e.g. the student or someone else might be harmed if you don't disclose)
- 1.4. The guidelines cover the disclosure of any individual's data, not just students. It is recommended that if you are in doubt you obtain advice from a Director. In all circumstances your first consideration should be what is in the interest of the data subject.

## **2. Confirmation of Student status**

2.1. Student status is regarded as personal data under Data Protection Legislation. Confirmation of whether or not an individual is a student of MetFilm is therefore considered to be unauthorised disclosure of personal data. If you are asked to confirm whether a named individual is a student of MetFilm you should offer to pass on any message without confirming or denying that the person is a student of MetFilm, or providing contact details. Suggested wording may be “if the person is a student of MetFilm I will pass on your details to them for them to contact you.”

## **3. Confirmation of employee status**

3.1. The same applies in relation to employees of MetFilm. Before disclosing personal information, you should always consider whether or not disclosure of the information is relevant to, and necessary for, the conduct of MetFilm business. For example, it would be appropriate to disclose a colleague’s work contact details in response to an enquiry relating to their work function. However, it would not be appropriate to disclose a colleague’s work details to someone who wished to contact them for non-work related matter

## **4. Circumstances where you may disclose personal information**

4.1. The following are examples of circumstances where you may disclose personal information in accordance with the principles of Data Protection Legislation

- 4.1.1. Where explicit consent has been given by the individual (data subject) (e.g. a student has signed a consent form for MetFilm to pass on their details to the external recruitment agency);
- 4.1.2. Where the disclosure is in the legitimate interest of MetFilm (e.g. A tutor has concerns regarding one of their student’s attendance and requests data relating to the student’s attendance);
- 4.1.3. Where MetFilm is legally obliged to disclose the data (e.g. HESA returns, ethnic minority and disability monitoring; UCAS);
- 4.1.4. Where disclosure of data is required for the performance of a contract (e.g. informing Student Loan Companies of academic progress, attendance and performance.);

## **5. Circumstances where you may disclose personal information WITHOUT the Data Subject’s consent:**

5.1. You may disclose personal information without the data subject’s consent ONLY in the following circumstances:

- 5.1.1. Where disclosure is necessary for safeguarding national security.
- 5.1.2. Where disclosure is necessary for the prevention or detection of crime,

including the apprehension or prosecution of offenders.

5.1.3. Where disclosure is necessary for the assessment or collection of tax or duty.

5.1.4. Where disclosure is necessary for the discharge of regulatory functions (including the health, safety and welfare of persons at work)

5.1.5. Where disclosure is necessary to prevent serious harm to the data subject or a third party.

5.2. Under these circumstances requests for disclosure of personal data MUST always be supported by appropriate paperwork. (e.g. official documentation stating that the information is required in support of an on-going investigation with the exception of condition 5 above (for the prevention of serious harm). Information regarding disclosure to the Police can be found in Appendix D.

## **6. Sensitive Personal Data**

6.1. Stricter conditions apply before sensitive personal data can be disclosed to third parties. Sensitive data is information relating to the following:

6.1.1. Race or ethnic origin

6.1.2. Political opinions

6.1.3. Religious beliefs

6.1.4. Trade Union membership

6.1.5. Health

6.1.6. Sex life

6.1.7. Criminal convictions or allegations of criminal conduct

6.2. Sensitive data should only be disclosed if one of the conditions in Schedule 2 (as set out above) AND one of the conditions in Schedule 3 are met. The most likely conditions of Schedule 3 applicable to MetFilm are:

6.2.1. The student or member of staff has given their written consent.

6.2.2. Disclosure is in the vital interests of the student or member of staff (e.g. information relating to a medical condition may be disclosed in a life or death situation).

6.2.3. Disclosure is necessary for legal advice or proceedings.

## **7. Emergencies**

7.1. Student/staff information can be disclosed in emergency situations where the

student/staff member or someone else's life or health and safety might be at risk. Please ensure a record is kept of what information was provided and why and provide a copy to a Director.

## **8. Sharing Information with staff members**

8.1. You may share personal data only on a 'need to know' basis within MetFilm. The question to consider before disclosing the information to colleagues is whether or not the information is necessary to allow the person to do their job. You must also consider whether the purpose for which the colleague wishes to use the personal data for is within MetFilm's notified purposes or consent has been provided by the data subject. If it is not, then you will require the consent of the data subject before you can disclose the information to the colleague. For example, a colleague from Marketing contacts you to request email addresses of graduates for the purposes of sending emails to graduates to participate in an advertising campaign on behalf of the business. You may not disclose the personal email addresses of graduates to Marketing without first obtaining consent from the graduates. As the purpose for which Marketing wish to obtain graduates personal details fall outside the original purposes for which the graduates had provided consent for disclosure of their personal information. In this instance, you may send an email on behalf of Marketing with details of their request to the graduates seeking consent as to whether they wish to have their personal details disclosed to Marketing.

8.2. If the information is sensitive personal data (e.g. disability or health information) you should not share it without the explicit consent of the data subject. This means that the data subject must be fully aware of who the information will be shared with and have given agreement to this. For example, you may pass on information to the graduation office regarding a student's disability needs to enable special arrangements to be made for the student to attend the ceremony only where the student has given consent for information to be disclosed about their disability.

## **9. External Disclosure Parents/Guardians/Friends**

9.1. Parents, guardians, other family members or friends have no special right to personal information about the student. MetFilm has no obligation or responsibility to disclose personal information to the student's relatives even if they are contributing to tuition fees if the student has not given consent for their information to be disclosed. If you disclose personal information without the consent of the student this will be a breach of Data Protection Legislation.

## **10. Eighteen or Under**

10.1. Where students are under eighteen years old, a member of staff may only contact a parent or guardian where that member of staff believes it is in the best interests of the student concerned to do so after full consultation with the student where possible. This contact may be in connection with the student's attendance, academic progress or performance and/or disciplinary proceedings for academic or non-academic offences.

10.2. No information about students over the age of 18 should normally be given to parents or guardians without the student's written permission.

## **11. Where Parents seeks to pay fines or fees**

11.1. If you confirm or inform parents or others of the amount owed this would involve a disclosure of student personal data. In these situations you have two options:

11.2. If you are able to verify the parent is acting on behalf of their son or daughter for example by asking for a reference number or the amount on an invoice you may confirm the amount and allow them to pay. You should not provide any further information (e.g. about the reason for a fine).

11.3. If it is not clear the parent is acting on behalf of their son or daughter you should be cautious and explain that we cannot normally provide information about fees etc. to other people, but they could arrange for their son or daughter to provide consent. Once you have the student's consent, it is acceptable to allow the parent to pay fees or fines.

## **12. Sponsor**

12.1. Where a formal sponsorship agreement exists between the student and sponsor, MetFilm may disclose the students' academic records relating to their progression, attendance and performance to sponsors. Sponsors may be employers, training providers, Student Loan Company, or Research Council. Where the sponsor is a parent and no formal sponsorship agreement exists between the student and parents, you should not disclose the student's academic record without first obtaining the student's consent.

12.2. No information about students other than on the basis set out above should normally be given to sponsors without the student's permission.

12.3. Whilst MetFilm may disclose the student's academic records without consent from the student provided there is a formal sponsorship agreement, it is good practice to ensure that the student has provided consent for the disclosure of their academic records to their sponsor.

## **13. Disclosure to the Police**

13.1. There is no compulsory requirement to disclose to the Police in the absence of a court order requiring information. There is an exemption in Data Protection Legislation which enables MetFilm to disclose information to the Police without the student's (data subject) consent. The exemption enables disclosure for the purposes of 'the prevention or detection of crime' and 'apprehension or prosecution of offenders'.

13.2. Requests by the Police are processed centrally by the Head of Registry. You should only disclose personal information about a student or staff member in an emergency situation and only if the Police have confirmed they need to speak to a named individual in connection with a criminal investigation and failure to provide the information would

prejudice the investigation. In all other circumstances you must forward the Police request to the Head of Registry

- 13.3. YOU should NOT release information to the Police over the telephone. Request for disclosure by the Police must be made in writing. Most Police forces will have their standard request form. The request must include a statement confirming that the information is required, a brief outline of the nature of the investigation, the student's or staff member's role in the investigation and the signature of a Director. This information should be provided to the Head of Registry.

#### **14. Council Tax**

- 14.1. There is no legal obligation to disclose student information to council tax officers, however, there is an exemption in Data Protection Legislation (the same exemption used for Police requests) to enable MetFilm to disclose information to the Council without the student's consent.
- 14.2. The exemption allows disclosure of personal information for the purposes of enabling the collection or assessment of tax. Requests by the council are processed centrally by the Head of Registry. If you receive a request for details of a student's personal information from the council forward the request to the Registry Team.

#### **15. UK Visa & Immigration (Previously UK Borders Agency)**

- 15.1. MetFilm has a legal obligation to disclose international students' personal data to the UK Visa & Immigration Agency. International students are advised that their personal information will be disclosed to the UK Visa & Immigration Agency at registration in the Student Terms & Conditions and consent is deemed to have been provided by the International student upon acceptance of the Terms and Conditions.
- 15.2. The UK Visa & Immigration Agency request for personal information should be made in writing either on headed paper or from an official email address. Where the request for information is by email, the email verification procedure should be followed. You need to:
- 15.2.1. Check the email is a valid address and that it is from an official email account;
- 15.2.2. Call the telephone number displayed on the email request to confirm the identity of the person requesting the personal data and that they are from the organisation they claim to be representing.
- 15.2.3. Once you are satisfied the request is genuine, you may respond by email to the request for personal information.
- 15.2.4. The request for information must be about a specific named individual.

#### **16. Child Support Agency**

- 16.1. The Child Support Agency has power to obtain certain information. This will depend

on what legal powers they are relying on. If you receive a request from the Child Support Agency, please provide the standard response set out in paragraph 21 below and refer the matter to the Head of Registry

## **17. Department of Work & Pensions/Job Centre Plus**

17.1. MetFilm is legally required to provide the DWP with information in some circumstances in relation to benefit fraud investigations. The request should specify these legal powers and explain why the information is required. Use standard response if unsure (see paragraph 21).

## **18. Local Education Authorities**

18.1. MetFilm has a statutory duty to disclose limited information such as students' registration status to the Local Education Authorities who assess an undergraduate students' eligibility for fees and loan agreements. Students are informed of MetFilm's disclosure obligation at registration.

18.2. Disclosures to the Local Education Authority should be limited to the facts. Sensitive data (e.g. health) cannot be disclosed to Local Education Authority without the student's consent.

## **19. Academic Partnership Arrangements**

19.1. Academic partnership arrangements with other colleges and educational providers would necessarily involve the sharing of student information. When sharing student information with partners it is important to ensure:

19.1.1. You only share the minimum amount of student information required

19.1.2. If any sensitive personal data is to be shared, you must ensure you have the student's consent

19.1.3. Information must be shared securely

19.1.4. You have agreed who will keep student information and for how long.

## **20. Disclosure to current and prospective employers and educational institutions**

20.1. MetFilm regularly receives requests for information about current or former students from potential or current employers and educational institutions conducting background checks for job or course applications. Although disclosure in these circumstances will usually be in the best interests of the student, you should still ensure that consent from the student has been obtained. The information disclosed should be kept to a minimum – usually registration status and/or award.

## **21. Work placements & Exchanges with other institutions**

21.1. Where students undertake work placements or exchanges with other institutions,

this will involve limited sharing of student personal data between MetFilm and the third party. Students should be made aware of such disclosure and requested to sign a consent form before the placement or exchange begins.

## 22. Survey/Research Organisations

22.1. You may be approached by surveys or research organisations for a list of student addresses or emails for them to market their services or circulate a survey. You must NOT provide this information but can offer to mail the information/survey on their behalf. If you do decide to undertake a host mailing, you should include a statement explaining the context of the mailing and reassure students that their personal data have not been released to the third party. You should also include an option for the student to opt out of receiving such mailings.

## 23. Standard response if uncertain if data can be provided to a third party

23.1. The following standard response should be used whenever you receive a request for personal data from a third party and you are uncertain whether you can provide the information.

23.2. Please adapt the wording as appropriate depending on the request for information.

“As you will understand, MetFilm has responsibilities under Data Protection Legislation to safeguard the information we hold in respect of our students. Please could you provide me with some further information as follows: -

- if you have the individual's consent to the disclosure please provide evidence for this (for example, a copy of the relevant section of an application form if applicable);
- if you have a statutory power to request the information, please provide details of the relevant legislative provision;
- if the disclosure is covered by an exemption under Data Protection Legislation, please could you quote this and explain why it is applicable.
- If there is any other reason why you feel MetFilm should provide the information you request, please could you provide further details”.

## Appendix D Using Personal Data for Direct Marketing

1. Under Data Protection Legislation an individual has the express right to object to the use of their personal data for direct marketing purposes. ‘Direct Marketing’ is defined in the Act as the communication of any advertising or marketing material which is directed to particular individuals.

2. It is best practice for the direct marketer to inform the Data Subject of this right, and the Information Commissioner expects this. MetFilm provides students with an 'opt- out' option on the Application and Enrolment forms allowing students to indicate their desire to exercise this right. If MetFilm direct markets to an individual who has exercised this right it is in breach of the Act. It is therefore important to check the student records before sending out any marketing material.
3. If an individual has exercised this right the only marketing material MetFilm could send them would be in response to a specific request. For example where a student has ticked the 'opt-out' box on their Enrolment form, and subsequently requests a part-time prospectus, in this case MetFilm could send a part-time prospectus, but no other material. Data collection forms where the data collected may be used for direct marketing must clearly state this. MetFilm must also inform the data subject of their right to prevent processing for direct marketing purposes. For example by including a phrase such as "We may wish to send you promotional/advertising material about our other courses/services. If you would prefer us not to do this please tick this box?"
4. Direct marketing by electronic means (i.e. by email or by SMS text message) is governed by different rules set out below.
5. If you intend to direct market an individual, who is not currently a student, by electronic means, they are required to opt in. MetFilm must provide the tick box as above, but the wording must read "We may wish to send you information or contact you about our other courses/services by email, phone or text message. If you would like us to do this please tick this box?"
6. If you intend to direct market via these media, to an individual who is already our student, information related to the service we already provide them then that is allowed. E.g. Texting an advert for a course to an individual currently studying with us. Assuming that student has not opted out when providing us their data.
7. In addition, any direct marketing that does take place must include a note stating that the marketing is from MetFilm and that individuals have a right to prevent processing for direct marketing purposes.
8. In order to fulfil our obligations to data subjects we must maintain up-to-date databases that allow us to remove or otherwise exclude individuals who have exercised their right to prevent processing. The Pardot database of student data is maintained as the most accurate record of students' wishes in this regard.

## Appendix E Reference Guidelines

### 1. Introduction

1.1. There is no specific legal obligation on MetFilm to provide a reference for an employee

or former employee as there is not a requirement in the contract of employment, but MetFilm could be subject to a claim for discrimination if it refused to provide a reference for reasons relating to sex, race or disability. Nevertheless, as a good employer, it is standard practice to give a reference to an employee upon request.

## 2. Accuracy of References Responsibilities of Staff

2.1. It is the duty of the referee writer to exercise reasonable care and skill in providing a reference. The writer should take reasonable steps to:

2.1.1. Ascertain that the information on which the reference is based is factually correct. Even if the reference writer honestly believes the inaccurate statements to be true, he/she may still be negligent if reasonable steps have not been taken to check the veracity of statements.

2.1.2. Check whether an agreed reference has been placed on the individual's file with the relevant Human Resources Adviser.

2.1.3. If the writer chooses to express opinions about the subject of the reference, they should ensure that the opinions expressed are reasonable in the circumstances and can be justified. Opinions are, by their very nature, subjective but they must be arrived at reasonably. The person expressing the opinion should always ask whether, if called upon to do so, he/she could justify why he/she holds those opinions – i.e. whether the opinion has a proper basis in fact. Statements of opinion should not be presented as statements of fact.

2.2. There is nothing to prevent the reference writer from showing the subject the reference before submitting it. Their consent will ensure compliance with Data Protection Legislation.

2.3. Create a fair impression overall. This might mean putting certain factual matters into context where not to do so would create a misleading impression. Having checked the factual accuracy of statements and the reasonableness of opinions contained in the reference, the writer should “stand back” and ensure that the effect of the whole reference is fair and not misleading. A reference writer who is negligent in the above respects will render MetFilm liable for any loss, which the employee incurs as a direct result of inaccurate statements, opinions or impressions.

2.4. Where the person providing the reference has limited knowledge of the subject, this should be clearly stated.

2.5. In appropriate cases MetFilm may make the provision of a reference conditional upon a disclaimer of liability to the subject and to the recipient.

2.6. Whilst it may sometimes be tempting to provide a reference that portrays the employee/student in a better light than is justified this should not be done since a reference which is unduly favourable could potentially leave MetFilm vulnerable to a claim for damages from the recipient of the reference.

### 3. "In Confidence"

3.1. Many references are written and received "in confidence". If, however, there is a claim for damages the reference may have to be disclosed. It should also be noted that references received would have to be disclosed in the event of a subject access request by the data subject. Reference writers need to be aware of this when drafting references.

### 4. Equality & Diversity and References

4.1. It is unlawful to discriminate on grounds of race, sex, disability, sexual orientation, religion or belief, part-time status, fixed term employment contract status or trade union membership or activity. It is specifically unlawful to instruct, procure, induce, comply with, or knowingly aid, an act of unlawful discrimination.

4.2. In giving references, care should be taken to avoid overt or covert, intentional or unintentional acts of unlawful discrimination. This is particularly the case where opinions not based on any objective evidence are sought or offered on the suitability of applicants. Opinions should, therefore, be capable of being backed up by objective evidence.

### 5. Access to references

5.1. MetFilm's Policy of allowing staff open access to their personnel file and the right of students under Data Protection Legislation to make a subject access request means that the references MetFilm receives will always be accessible to the subject. Reference request forms sent out from MetFilm should therefore make this clear to the referee.

## Appendix F Examinations and Assessments

In general, students are entitled to all personal data relating to the exam and assessment process. However, there are a number of exemptions which apply in some circumstances: -

### 1. Examination/coursework results

1.1. Students are entitled to information about their exam results and assessment marks. However, they are not entitled to this information before the normal publication process. If a student makes a Subject Access Request for this information prior to the official publication of exam results, you have five months in which to provide the information (this allows time for the marks to be published by the time the request is answered) or forty days following the publication of the results, whichever is the shorter.

### 2. Examination Scripts

2.1. Exam scripts (or other written assessments) are exempted from Subject Access Requests. This means that MetFilm is NOT obliged to provide students with copies of

exam scripts.

### **3. Examiners Comments**

3.1. Although exam scripts are exempt from disclosure, comments made by examiners are not. This means students are entitled to see any comments made by internal or external examiners. Where comments are made on the actual examination script and the department chooses not to disclose the script, the examiners comments must be reproduced onto a separate form. It must be in an “intelligible form”. It is therefore recommended that comments be made on attached sheets rather than directly on examination scripts.

3.2. Examiners are reminded that their comments are disclosable to students, all comments need to be justified and no careless remarks should be made on exam scripts, in emails/memos to colleagues or on mark sheets. Any informal notes made in the course of marking an examination script or coursework should be securely disposed of once the final mark has been agreed and there is no genuine need for the notes to be retained.

### **4. Examination board minutes and related documentation**

4.1. Any references to identifiable students in examination board minutes or similar documents will be disclosable to students under Data Protection Legislation

### **5. Publication & Release of Results**

5.1. Examination results, (which include coursework marks, module marks and interim tests) are personal data and therefore should not be disclosed to third parties without consent. Where MetFilm publishes results for example via public notice-boards, Graduation Programme, or announcements of results including classification at graduation ceremonies, MetFilm has an obligation under Data Protection Legislation to notify students prior to the publication and provide a mechanism through which they can object to their results being displayed in all or any particular form. Registry will undertake to email students to explain, where, and how, students may expect to see their results published and to advise MetFilm if they do not wish to have their results published accordingly.

## **Appendix G Telephone Guidance**

These guidance notes are intended to provide guidance for staff who deal regularly with telephone calls from third parties requesting personal data on students and staff.

### **1. Internal disclosure within MetFilm by Telephone**

1.1. Care must always be taken before disclosing student or staff personal information to work colleagues regardless of whether they are within or external to your department.

- 1.2. Data Protection Legislation only allows you to disclose personal data to colleagues if they have a “legitimate interest” in the data concerned. However, no definition of “legitimate interest” is provided within Data Protection Legislation, you will therefore need to determine on a case by case basis whether they have a legitimate interest by asking the question “whether or not the information is necessary to enable them to perform their job”. You should also consider the level of detail disclosed which is necessary for them to perform their job.
- 1.3. Before consideration of the “legitimate interest” criteria, you must be satisfied that consent has been provided by the Data Subject for the purpose(s) to which the request is based on. Where the Data Subject is a student consent may be provided in the Student Terms and Conditions or other consent forms.
- 1.4. Provided you are satisfied with the above, in the event where you are able to identify the member of staff over the telephone from their voice and you are satisfied they have a legitimate reason for making a request for the personal information, you may disclose over the telephone. Please ensure that when disclosing the information over the telephone you are not inadvertently disclosing the information to other members of staff. This is particularly important in the case of sensitive personal data and when working in an open plan office.
- 1.5. If you are unsure of the identity of the member of staff making the telephone enquiry, you should ask them to put the request in writing by email. Keep the written request as background evidence should the disclosure be questioned at a later stage.

## **2. External Disclosure outside MetFilm by Telephone General**

- 2.1. In general, personal information should not be disclosed over the telephone EXCEPT in exception circumstances or emergencies, where the health or welfare of the Data Subject is at stake.
- 2.2. It is strongly advised that you ask enquirers to submit their request in writing (where appropriate on headed paper). This will enable you to check whether or not the request is legitimate and where appropriate obtain consent for the disclosure from the Data Subject. You should reply to the request in writing where ever possible.

## **3. Exceptional Circumstances**

- 3.1. In exceptional circumstances such as emergencies, time constraint and other factors it may be necessary to disclose information over the telephone. Information may only be given over the telephone or to personal callers after establishing the true identity of the caller e.g. by using dial-back or taking a telephone number and calling the individual back and by asking security questions to confirm the following information about the Data Subject
  - 3.1.1. their unique identifier (UCAS no, staff or student number),
  - 3.1.2. name

3.1.3. address

3.1.4. data of birth

3.2. Before you disclose the personal data, you should take a contact number and ring the enquirer back to ensure the caller is who they say they are.

3.3. A written note of the information disclosed must be sent to a Director.

#### **4. What to do if someone calls claiming to be a student**

4.1. You may receive telephone calls from individuals claiming to be students and asking, for example, for their examination results. Unless you are 100% sure that the person on the line is who they claim to be, you should not disclose information over the telephone. You should ask security questions (as set out above) to confirm their identity before proceeding with the call.

## **Appendix H Funding Body Purposes**

MetFilm is required to provide statistical information on its students and staff to its funding bodies, Higher Education Statistics Agency (“HESA”), The Skills Funding Agency (“SFA”), and Health Education England.

### **1. Higher Education Statistics HESA**

1.1. Some information about students held by MetFilm will be sent to the Higher Education Statistics Agency (“HESA”). Student records will be added to a database which will be passed to the central government departments and agencies and devolved administrations which require it to enable them to carry out their statutory functions under the Education Acts. It will also be used in anonymised form for statistical analysis by HESA and the above bodies resulting in publication and release of data to other approved non-statutory users. These may include academic researchers and commercial bodies.

1.2. Students may wish to note that their contact details will not be made available to HESA, their names will not be used or included in its statistical analysis and precautions are taken to minimise the risk that individual students will be able to be identified from the data. Neither statutory nor non-statutory users of the HESA data will be able to use the data to contact students.

1.3. Under Data Protection Legislation students have the right to a copy of the data held about them by HESA, for a small fee. If students have any concerns about, or objections to, the use of data for these purposes, they should contact HESA at [www.hesa.ac.uk](http://www.hesa.ac.uk) or by writing to 18 Royal Crescent, Cheltenham, GL50 3DA.

### **2. The Skills Funding Agency - The SFA have asked us to provide the following information for**

learners:

- 2.1. The information you provide on the enrolment form will be passed to the Skills Funding Agency. The SFA is responsible for funding and planning education and training for over 16-year-olds in England, and is registered with the ICO. The information you provide will be shared with other organisations for the purpose of administration, careers and other guidance and statistical and research purposes. Other organisations with which we will share information include, the Department for Education and Skills, Connexions, Higher Education Statistics Agency, Higher Education Funding Council for England, educational institutions and organisations performing research and statistical work on behalf of the SFA or its partners. The SFA is also a co-financing organisation and uses European Social Funds from the European Union to directly or indirectly part-finance learning activities, helping develop employment by promoting employability, business spirit and equal opportunities, and investing in human resources. Further information about partner organisations and what they do, may be found at <https://www.gov.uk/government/organisations/skills-funding-agency> and by following the links to data protection.
- 2.2. At no time will your personal information be passed to organisations for marketing or sales purposes. From time to time students are approached to take part in surveys by mail and phone, which are aimed at enabling the SFA and its partners to monitor performance, improve quality and plan future provision.

### **3. Staff Collection Notice**

- 3.1. Some information held about staff by MetFilm is sent in coded and anonymised form to the Higher Education Statistics Agency (HESA) annually and to the Skills Funding Agency ("SFA"). Staff records are added to a database which is passed to central government departments and agencies and devolved administrations which require it to enable them to carry out their statutory functions under the Education Acts. It is also used for statistical analysis by HESA, the SFA and the above bodies resulting in publication and release of data to other approved non-statutory users. These may include academic researchers and unions.
- 3.2. Staff may wish to note that their name and contact details will not be made available to HESA or the SFA and precautions are taken to minimise the risk that individual staff will be able to be identified from the data.
- 3.3. Under Data Protection Legislation staff have the right to a copy of the data held about them. Because the data held about staff by HESA and the SFA is anonymised and a subset of that held on staff by MetFilm, data subject access requests should be addressed in the first instance to MetFilm. If staff have any concerns about, or objections to, the use of data for these purposes, they should contact HESA at [www.hesa.ac.uk](http://www.hesa.ac.uk) or by writing to 18 Royal Crescent, Cheltenham, GL50 3DA or the SFA using the contact details given above.