



# Data Protection Policy

## Introduction

---

1.1. Brighton Film School has to collect data about its members of staff, students, clients and other users to allow it to monitor performance, achievements, health and safety and security. It is also necessary to process this data so that staff can be paid, courses organised, and legal obligations to funding bodies and government complied with.

1.2. Data also enters the public domain through social networking sites and emails. Therefore, the security of data transferred via these methods is also subject to the data protection principles.

1.3. In managing data on a day-to-day basis, Brighton Film School will adhere to the data protection principles prescribed by the Data Protection Act 1998 and associated legislation.

## Scope of this Policy

---

2.1. This policy will not form part of the formal contract of employment but it is a condition of employment that members of staff will abide by the rules and policies made by Brighton Film School. Any failure to follow the policy can result in disciplinary proceedings.

2.2. Any member of staff who considers that the policy has not been followed in respect of the data held about them should raise the matter with the Business Manager initially. If the matter is not resolved, it should be raised as a formal grievance.

## Personal Data

---

3.1. All personal data shall:-

- Be obtained and processed lawfully and fairly. Processing will not be carried out unless certain conditions are met.
- Be obtained for a specific and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for the purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for the purpose (refer to the Retention of Documents guide).
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or damage.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection of personal data or consent has been given.

## Notification of Data Held and Processed

---

4.1. All staff, students, clients and other users are entitled to: -

- Know what information Brighton Film School holds and processes about them and why.
- Know how to gain access to the stored data.
- Be aware of the procedures in place to keep the data up to date.
- Know what Brighton Film School is doing to comply with its obligations under the Data Protection Act and associated legislation.

4.2. The Business Manager will provide every member of staff with a standard form of notification annually showing the items of personal data that are stored on the database.

## Responsibilities of Staff

---

5.1. All staff will be responsible for: -

- Fully complying with the Data Protection principles (3.1) in their handling of personal data.
- Performing a Privacy Impact Assessment where new processing of personal data is planned.
- Promptly raising concerns about Data Protection or Data Security with the Business Manager.
- Ensuring that all data that they provide to Brighton Film School in connection with their employment is accurate and up to date and that changes are notified to the Business Manager using the appropriate forms.
- Checking the information that Brighton Film School holds annually and correcting any errors.

5.2. Any personal details of other people collected by a member of staff such as coursework marks or grades, references to employers or other academic institutions, or any matters about personal circumstances must be collected and stored in accordance with the guidelines included in the Staff Handbook and with the Data Protection Policy.

## Data Security

---

6.1. Staff are personally responsible for ensuring that:-

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

6.2. All personal data must be kept in a locked filing cabinet or drawer. If it is stored on a computer, it must be stored securely with access only available to those who require it. Holding personal data on removable media or mobile devices is discouraged and the use of encryption is mandatory in these cases.

6.3. Students must ensure that all data supplied to Brighton Film School is accurate and up to date. Any changes in the data must be notified to the Business Manager.

## Data Security

---

7.1. Persons on whom Brighton Film School holds data have the right to access any of the personal data that is stored about them either on a computer or in certain physical files. Some suggested categories of information are provided in Annex

A. The request must be made in writing to the Business Manager and accompanied by both a proof of identity (see Annex B) and a cheque for £10 made payable to Brighton Film School. The

request must include enough information to enable Brighton Film School to find the personal data being requested.

7.2. Brighton Film School will aim to comply with all requests for information as quickly as possible but will ensure that in all cases the details are provided within 40 days.

7.3. Personal Information will never be disclosed over the telephone to outside bodies, or internal staff other than appropriate managers.

## Publication of Information

---

8.1. It is the policy of Brighton Film School to make as much information public as possible. The following will be available to the public for inspection:-

- Names and photographs of the members of the Management.
- Summary details of student achievement and examination successes. Details relating to an individual student will not be published without the express permission of that individual.
- Student participation in productions and events related to or resulting from their studies. Again, the permission of the individual would be obtained before this was done.

8.2. Brighton Film School's internal phone list will not be a public document.

8.3. Any data subject who has good reason for wishing that any of these details should remain confidential should contact the Business Manager.

## Subject Consent

---

9.1. In accordance with the Data Protection Act 1998, Brighton Film School will obtain consent from future students and new members of staff for the collection and processing of data. For the items described in the Act as sensitive data, express consent will be obtained. This will include information about previous convictions and health needs. In cases where the applicants will be in contact with children and young people between the ages of 16 and 18, checks will be made, in accordance with the relevant statutes, to ensure that the people are suitable to work at Brighton Film School.

9.2. Enrolment and staff appointments will therefore become conditional on this consent being given.

## Processing Sensitive Information

---

10.1. For the purposes of operating the sick pay, equal opportunities, and other policies it is necessary to process sensitive information about a person's health, previous convictions, protected characteristics (such as race, ethnicity or disability), and other family details. Brighton Film School is aware that this could cause particular concern or distress.

10.2. Explicit consent is required prior to the collection and processing of sensitive personal data.

## Data Processor

---

11.1. A 'Data Processor' is someone who carries out processing (which can be just viewing or holding) of personal data on the behalf of Brighton Film School.

11.2. There must be a contract in place stipulating equivalent levels of protection for personal data as those implemented by Brighton Film School and stipulated by the Data Protection Act.

## Data Controller

---

12.1. The Chief Executive is ultimately legally responsible for the implementation of the Act.

12.2. Brighton Film School has two Data Controllers and these are the Chief Executive and the Head of School who will designate other members of staff to deal with day-to-day matters.

## Examination Marks

---

13.1. Students will be given information about their marks or grades for coursework and examinations. Brighton Film School may withhold enrolment, awards, certificates, accreditation or references in the event that monies are due to the School.

## Retention of Data

---

14.1. Brighton Film School will keep some forms of data longer than others. However, information about staff and students cannot be kept indefinitely.

14.2. Brighton Film School will maintain a separate retention policy listing key categories of data and how long they will be retained.

14.3. Any data reaching the end of its retention period will be securely and permanently disposed of. This will include both computer files and physical documents.

14.4. Any electronic media containing personal data must be securely disposed of at the end of its useful life.

14.5. Student records will be kept for a period of seven years from when the student leaves the School. Student records include certain sensitive information that we are required to collect by Government funding bodies. This information includes ethnic origin and may include details relating to personal status. Further details may be obtained from the Business Manager.

14.6. Staff records will be kept for a period of seven years after the member of staff leaves the School. Information concerning pensions, taxation, potential or current litigation regarding the employment and details required for references will be kept for longer periods as determined by the specific circumstances. Documents related to health and safety issues will be kept indefinitely.

## Cookies and similar technologies

---

15.1. Cookies are small pieces of data that are downloaded to a computer by a web site and allow the computer to be recognised by the web site on subsequent visits. They are often used for tracking of visitor activity or short-term uses such as maintaining shopping carts.

15.2. Newly amended legislation requires that consent is sought for the use of cookies for some purposes. The legislation covers not only cookies but any technology, which may leave data on a person's computer.

15.3. Any use of cookies or similar technology on externally facing Brighton Film School web sites must be assessed against the legislation to decide whether consent from visitors is required.

## Release of Personal Data to official bodies

---

16.1. Occasionally official bodies such as the Police or Inland Revenue may request the disclosure of personal information. Except in emergencies, this will be referred to the Data Controller or a person designated by the Data Controller and assessed against the relevant sections of the Data Protection Act.

16.2. There is an expectation that official bodies will provide a suitably authorized DPA Section 29 exemption form when requesting personal data from the School.

## Privacy Impacts Assessments

---

17.1. A Privacy Impact Assessment is essentially a risk management process and must be carried out prior to any new uses of personal data in order to identify any issues related to Data Protection or related legislation.

17.2. Privacy Impact Assessments must be formally documented and signed off by a person designated by the Data Controller prior to any new uses of personal data.

17.3. A Privacy Impact Assessment is a mandatory stage in the pre-planning of any new project involving use of personal data or any case where data is going to be processed by another company on behalf of the School irrespective of 17.2. In the event of a query about whether a Privacy Impact Assessment is required then please contact the person designated for Data Protection queries by the Data Controller.

## Marketing use of Personal Data

---

18.1. Any use of personal data for marketing purposes must comply fully with the Data Protection Act and the Privacy and Electronic Communications Regulations.

18.2. Any requests for permission to market to an individual must be made on an “opt in” basis.

## Links to other policies

---

19.1 The Information Security policy defines specific requirements in terms of data security.

19.2. The Social Networking Policy provides guidance related to data protection whilst online.

## Further Information

---

20.1. For further information on the Data Protection Act 1998, refer to the guidelines on the Intranet or on the Information Commissioner’s Office website.

## Status of this Policy

---

21.1. The policy was approved by the Chief Executive in January 2015.

21.2. The operation of this policy will be kept under review by the Chief Executive.

21.3. It may be reviewed and varied from time to time by the Chief Executive.

21.4. This policy has been equality impact assessed to ensure that it does not adversely affect staff.

Date approved: January 2015

Approved by: Chief Executive

Date reviewed: January 2015

Date for review: January 2016

## Appendix A

### Suggested categories of information

#### For staff

- Academic or employment references
- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information

#### For students

- Academic marks or course work details
- Academic or employment references
- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information

## Acceptable forms of identification

In order to verify the identity of a person requesting personal information one form of identification from each category must be provided.

### Photo identity

- Driving license
- Passport
- Forces identity card

### Proof of address

- Recent bank statement or utility bill etc