

May 2018

# Data Protection Policy



Last reviewed 15 May 2018

# Data Protection Policy

## Contents

<b>Data Protection Policy</b>	<b>3</b>
1 Background	3
2 The principles for processing personal data	3
3 Notifications of Data Held and Processed	4
4 Staff Responsibilities	4
5 Data Security	4
6 Right to Access Information	4
7 Subject Consent	5
8 Examination Results	5
9 Retention of Data	5
10 Monitoring for Compliance	6
<b>Appendix One</b>	<b>7</b>
<b>Data Protection Procedure Guidelines</b>	<b>7</b>
Background	7
1 Collecting Personal Data	7
2 Handling, Collecting, Processing and Storing Personal Data	7
3 Subject Access and Subject Rights	8
4 Archiving of Information	8
Other Definitions and Notes	8

# Data Protection Policy

## 1 - Background

1.1. The European Union's General Data Protection Regulation (GDPR) succeeds the UK Data Protection Act on 25<sup>th</sup> May 2018. Application of its requirements is mandatory. It is therefore essential that the club fully complies with its objectives, not just to avoid prosecution and bad publicity, but to demonstrate that the club operates with due diligence and responsibility. The GDPR covers both electronic and paper-based material.

1.2. The club needs to keep certain information related to employees, members and other such type information in order to monitor

- performance
- achievements
- health and safety

It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. The personal data of club members needs to be collected and processed in order to keep members up to date with club affairs and provide notice of members' meetings etc. To comply with the law, information must be fairly obtained, maintained, stored, used and passed on, only in strict accordance with the GDPR and the Data Protection Principles. These principles are listed within this document.

1.3. The Club Secretary is responsible for ensuring the implementation and monitoring of this policy and the associated Data Protection procedures. The club has designated the Office Manager as the person who is responsible for dealing with the operational implementation of this procedure.

## 2 - The principles for processing personal data

2.1. The GDPR has six Data Protection Principles. These specify that personal data must be

- 1 Processed fairly and lawfully and in a transparent manner in relation to the data subject
- 2 Obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- 3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- 4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
- 5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is being processed.
- 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.

In addition, the club as data controller, must be responsible for, and be able to demonstrate compliance with all of the above principles

2.2. The club and all staff, volunteers or others who process or use any personal information, must ensure that they follow these principles at all times. In order to ensure this happens, the club has developed this Data Protection Policy.

2.3. Personal data is defined in the GDPR as:

Any information relating to an identified or identifiable person (known as the data subject). This may be a name, identification number, location data or an online identifier.

## 3 - Notifications of Data Held and Processed

3.1. All members, employees, volunteers, service users and other users are entitled to know

- what information the club holds and processes about them and why
- the lawful basis on which it is processed
- the period(s) of data retention
- how to gain access to it
- how to keep it up to date
- what the club is doing to comply with its obligations under the regulation

3.2. The club will make available a privacy notice to all data subjects which explains their individual rights as well as the means by which it complies with the requirements of the regulation.

3.3. The club will provide employees and volunteers with guidelines, which will be included in each new starter pack, issued on induction. This will state all the types of data the club holds and processes and the reasons for which it is processed. This will also provide guidance in carrying out and complying with the regulation.

## 4 - Staff Responsibilities

4.1. Staff are responsible for

- checking that any information that they provide to the club in connection with their employment is accurate and up to date
- informing the club of any changes to information, which they have provided i.e. changes of address or telephone number
- checking the information that the club will send out from time to time, giving details of information kept and processed about staff
- informing the club of any errors or changes. The club cannot be held responsible for any errors unless the member of staff has informed the club of any errors and provided the correct information to be used

4.2. If and when, as part of their responsibilities, staff collect information about other people, they must comply with the guidelines.

## 5 - Data Security

5.1 All staff are responsible for ensuring that

- any personal data, which they hold, is kept securely
- personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

5.2. Staff should note the unauthorised disclosure may be regarded as a disciplinary matter and dealt with accordingly.

## 6 - Right to Access Information

6. Members, employees, volunteers and service users have the right to access any personal data that is being kept about them on computer or in certain files. Any person who wishes to exercise this right should complete the club's Request for Information form and send it to the Club Secretary

6.2. The club aims to comply with the requests for access to personal information as quickly as possible, but will ensure that it is provided within one month from the date of the request being made, unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

6.3. The club will not make a charge for responding to such a request unless the request is manifestly unfounded or excessive, particularly if it is repetitive. It reserves the right to charge a reasonable fee for requests for further copies of the same information.

6.4 The identity of the requestor must be established before the disclosure of any information. Evidence of identity can be established by requesting production of:

- Passport
- Driving licence
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

*This list is not exhaustive.*

## 7 - Subject Consent

7.1 For the club to undertake any marketing communications with data subjects the express consent of each individual is required. The individual will be informed of their right to withdraw this consent to receive marketing communications at any time, and how to withdraw this consent.

If the personal data collected is sensitive, express consent for processing must be obtained (except in the case where processing of such data is a condition of employment – see clause 7.2 below). Sensitive personal data (or 'special categories of personal data') is defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning a person's health, sex life or sexual orientation.

7.2 In the case of the recruitment process and an offer of employment sensitive personal data will only be obtained when strictly necessary. The individual will be informed of the types of data obtained for the club to carry out its obligations and rights as an employer but consent will not be obtained.

7.2. Some jobs or projects will bring the applicants into contact with children, including young people between the ages of 14 to 18. The club has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The club also has a duty of care to all staff, members, volunteers and service users and must therefore make sure that employees and volunteers do not pose a threat or danger to other users.

7.3. All volunteers will be asked to consent to their data being processed when an offer of a voluntary role is made. A refusal to sign such a form may result in the offer being withdrawn. In the case of children under the age of 16 the consent will only be considered valid if given or authorised by the holder of parental responsibility over the child.

## **8 - Examination Results**

8.1. Students on accredited courses will be entitled to information related to their marks or grades for both coursework and examinations as part of their tutorial support. This is within the provisions of the regulation relating to the release of data. However, this may take longer than other information to provide.

## **9 - Retention of Data**

9.1. The storage of information is necessary to comply with legal and audit requirements. There is a requirement for a managed process when retaining documents. The club needs to ensure that personal details are not kept longer than necessary.

9.2. The retention of information and documents will be managed through the archiving system. In general, if information to be archived is not required because of legal, strategic or sound business reasons, then there is no requirement to keep it. There are very few circumstances to keep documents where there is no legal requirement to do so.

9.3. Electronic systems for retaining information are being developed. These systems are to be used primarily.

9.4. The club will keep some forms of information for longer than others. Because of restrictions in storage capacity, information cannot be kept indefinitely, unless there are specific requests to do so. A retention list is provided for detailing the retention periods. In general, the only records that the club will retain are listed in 9.5.

## 9.5 Retention Periods

<b>Type of Data</b>	<b>Retention</b>	<b>Description</b>
Personnel files, Training record, medical, etc.	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms, interview notes	6 months from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20)	3 years from the date of Redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more)	12 years from the date of redundancies	Limitation period for litigation
Income Tax and NI returns	3 years after the end of the financial year to which the records relate	Income Tax (Employment Regulations 1993)
Statutory Maternity Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulation 1986
Statutory Sick Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and Salary Records	6 years from the end of employment	Taxes Management Act 1970
Records and Reports of accidents	3 years after the date of the last entry	RIDDOR 1995 - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health	40 years	COSHH Regulations 2002
Student records, to include enrolment forms and records of achievement	Two academic years from the last date of the course. At the end of the specified retention period the Estates Department will be responsible for ensuring the appropriate and confidential disposal of documents	Audit requirements
Players medical records and fitness data	6 years	Provision of references and limitation period for litigation

## 10 - Monitoring for Compliance

10.1. The club will put procedures in place including a schedule of monitoring for compliance with the GDPR. The Club Secretary will put in place an annual schedule to ensure that there is routine monitoring for compliance with the regulation.

# **Appendix One**

## **Data Protection Procedure Guidelines**

### **Background**

The club will collect a variety of data, either personal, financial or student record related. These procedures are to be used by staff as a guideline for ensuring that all areas of the club operate within the GDPR. Managers are responsible for ensuring that current and all new processes and procedures take account of the requirements of the regulation.

### **1 Collecting Personal Data**

1.1. When collecting personal data make sure that people know

- who you/we are
- what the data will be used for
- to whom it will be disclosed

This should be done by issue of the privacy notice. It is important not to collect more personal data than is actually needed.

### **2 Handling, Collecting, Processing and Storing Personal Data**

2.1. When handling, collecting, processing or storing personal data, ensure that

- all personal data is both accurate and up to date
- errors are corrected effectively and promptly
- the data is deleted/destroyed when it is no longer needed
- the personal data is kept secure at all times (protecting from unauthorised disclosure or access)
- the Data Protection Act is considered when setting up new systems or when considering use of the data for a new purpose. Note that this may affect the existing registration with the Data Protection Authority
- written contracts are used when external bodies process/handle the data explicitly specifying the above requirements with respect to the data

2.2. It is equally important not to

- access personal data that you do not need for your work
- use the data for any purpose it was not explicitly obtained for
- keep data that would embarrass or damage the club if disclosed (for example, via a subject access request – see below)
- transfer personal data outside of the European Economic Area unless you are certain you are entitled to or consent from the individual concerned has been obtained
- store/process/handle sensitive personal data (see below) unless are certain you are entitled to or consent from the individual concerned has been obtained

2.3. Personal information should be

- under lock and key



- under personal supervision
- password protected if it is computerised
- kept only on other media which is itself secure

### 3 Subject Access and Subject Rights

3.1. Individuals, who the data relates to, have various rights

- to receive on request (a subject access request) details of the processing relating to them. This includes any information about themselves including information regarding the source of the data and about the logic of certain fully automated decisions
- to have any inaccurate data corrected or removed
- in certain circumstances to stop processing likely to cause substantial damage or substantial distress
- to prevent their data being used for advertising or marketing
- not to be subject to certain fully automated decisions if they significantly affect him/her

3.2. When a subject access request is received, it is important to

- treat the requestor with courtesy and try to understand what exactly is being sought
- act promptly and effectively as certain time scales are imposed regarding response

### 4 Archiving of Information

4.1. In general the only data that the club will retain and archive are outlined in the Data protection Policy under the Retention of Data section.

4.2. Managers are responsible for ensuring that all staff comply with the requirements of the Data Protection Policy and note is taken of them when designing and implementing new processes and procedures.

4.3. Staff must ensure that all records detailed in the Retention of Data section of the Data Protection Policy are archived in a timely manner.

### Other Definitions and Notes

Sensitive Data means data pertaining to

- racial or ethnic origin
- religious or philosophical beliefs
- trade union membership
- health, sex life or sexual orientation
- political opinions

This data may only be held in strictly defined situations or where explicit consent has been obtained. Data Controller is a person who determines the purposes for which, and the manner in which, any personal data is, or is to be, processed.

Subject Access is the right of individuals to have access to the data about them and other related information.