Data Protection Policy	
Date of adoption by British Gymnastics Foundation Board	12th June 2018
Last review date	

Summary of changes introduced at last review
Policy review cycle set to 3 years: Date of next review is June 2021. (This 3 year review cycle was agreed at the BGF Board on March 11th 2019)

CONTENTS

1. BACKGROUND

1.1 The Policy is informed by the General Data Protection Regulation (GDPR) which came into force on the 25th May 2018 and all other applicable laws and regulations relating to processing of personal data and privacy (described collectively as data protection laws).

1.2 Data protection laws all require that the personal data is processed in accordance with specific data protection principles. New data protection law provides stronger rights for individuals to be informed about how organisations use their personal data and greater control over how their personal data is used.

1.3 Data protection laws in the UK are regulated by the Information Commissioner's Office (ICO). The ICO has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher. Data protection laws can be enforced in the courts and lead to criminal sanctions. the courts have the power to award compensation to individuals. The ICO can also take a range of other enforcement actions and have powers of entry and seizure that may be used investigating organisations. The ICO can also audit organisations and required documentation to be provided that demonstrates how the organisation is accountable under data protection law. Assessments, investigations and enforcement action by, and complaints to, the ICO often become public knowledge and not only can they cause significant disruption to an organisation but can also damage an organisation's reputation and brand.

1.4 The Policy identifies our responsibilities under the data protection laws and the steps we will take not just to meet legal requirements but to build a culture of privacy and transparency where individual rights and freedoms are always at the forefront of everything we do with personal information.

2. PURPOSE

2.1 This policy interprets how our staff and volunteers who are acting as agents of British Gymnastics Foundation must comply with data protections laws in the context of work or voluntary activities for

British Gymnastics Foundation. It also applies to contractors delivering services for British Gymnastics Foundation.

2.2 The key aims of the policy are to: -

2.2.1 Identify our legal responsibilities under data protection laws and how we will comply;

2.2.2 Set out specific roles and individual responsibilities;

2.2.3 Ensure all staff and volunteers understand the importance of maintaining privacy and respecting individual rights and freedoms in relation to their personal data; and

2.2.4 Provide clarity and establish uniformity in data protection practice.

3 SCOPE

3.1 This policy covers all personal information we hold about employees, job applicants, temporary and agency workers, contractors, volunteers, beneficiaries, customers and anyone else whose data we process.

3.2 This policy applies to both personal data and sensitive personal data that is held in an automated (electronic) format. This includes:

3.2.1 All electronic devices, including desk top computer, laptops and tablets

3.2.2 Voicemail and call recordings

3.2.3 Text messages and any other personal information held on company devices

3.2.4 Imagery (photographs and video footage)

3.3 The policy also applies to manual filing systems where personal data are accessible according to specific criteria e.g. name, ID etc.

4 POLICY STATEMENTS

4.1 British Gymnastics Foundation is committed to complying with data protection laws and respecting the privacy rights and freedoms of individuals. We believe that ensuring personal information is processed in lawfully, fairly and transparently is of matter of strategic importance and a key departmental responsibility.

4.2 It is vital for the growth and sustainability of our organisation to maintain the trust and confidence of our staff, volunteers, beneficiaries and others whose data we process.

4.3 We recognise our responsibilities under data protection laws and will comply with the following data protection principles and ensure that any personal data is:

4.3.1 Processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

4.3.2 Collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes (purpose limitation);

4.3.3 Adequate and relevant, and limited to what is necessary to the purposes for which it is processed (data minimisation);

4.3.4 Accurate and where necessary kept up to date;

4.3.5 Kept for no longer than is necessary for the purpose (storage limitation); and
4.3.6 Processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures (integrity and security).

4.4 In addition, we recognise the we are required to demonstrate how we are accountable for complying with these principles and will:

4.4.1 Maintain a register of all personal data assets we hold;
4.4.2 Minimise the access to personal data to only those individuals who need the information to undertake their roles;
4.4.3 Maintain and implement a retention schedule for all data assets;
4.4.4 Only process personal data where we have a lawful basis to do so and it is necessary for the specific purpose;
4.4.5 Before relying on legitimate interests as a lawful basis, assess whether the processing can be achieved in a balanced way that safeguards individual interests, rights and freedoms.
4.4.6 Only process sensitive personal information where there is a lawful basis for doing so and an additional condition for processing sensitive information applies;
4.4.7 Only process criminal offences and convictions information where we have a legal obligation to do so and in accordance with our Policy on the Use of Criminal Record Checks;
4.4.8 Provide transparent information to all data subjects, including those who are children or otherwise vulnerable about the processing we undertake and their individual rights in a concise, intelligible and easily accessible form, using clear and plain language;
4.4.9 Ensure we have effective systems and processes to enable data subjects to easily assert their individual rights;
4.4.10 Implement appropriate technical and organisational measures to keep personal information secure, minimising the likelihood of unauthorised or unlawful processing and protecting against accidental loss, destruction or damage;
4.4.11 Where we determine the purpose(s) and means of the processing jointly with another data controller, ensure we agree and clearly document the respective liabilities and responsibilities and under data protection law;
4.4.12 Ensure that any individual or organisation who processes data on our behalf signs a contract/data processing agreement that provides sufficient guarantees that the processing is carried out in a way that meets all the requirements of data protection laws;
4.4.13 Ensure that where we undertake a processing operation on behalf of another controller we implement appropriate technical and organisational measures to maintain the security and integrity of their data and process it in accordance with applicable data protection laws;
4.4.14 Maintain a record of processing activities (RoPA) for all regular processing activities, those that involve sensitive personal data (special categories of personal data or criminal convictions and offences) and any processing that could result in a risk to the rights and freedoms of data subjects;
4.4.15 Maintain additional documentation as required to demonstrate our accountability under data protection laws;
4.4.16 Document and continually monitor the security measures in place for all personal data we hold and ensure they continue to provide an appropriate level of security paying due regard to the specific risks associated with the processing;
4.4.17 Take timely action to contain any personal data breaches and notify the Information Commissioner and affected data subjects where required to do so under data protection laws;

4.4.18 Undertake Data Protection Impact Assessment (DPIA) prior to undertaking a new processing activity that is likely to result in a high risk to the rights and freedoms of individuals and/or involves the introduction of a new technology;

4.4.19 Appoint a Data Protection Officer (DPO) who will be involved, properly and in a timely manner in all issues which relating to the protection of personal data;

4.4.20 Not transfer data outside the European Economic Area (EEA) except where it is permissible under data protection laws;

4.4.21 Ensure all staff, volunteers and contractors are provided with training that is appropriate to their role and responsibilities as set out in this policy; and

4.4.22 Take appropriate action against any individual who fails to comply with the policy, procedures and operational guidance.

5 DEFINITIONS

The following are the key definitions and terms used in this policy:

5.1 **Personal data/information** means any information relating to an identifiable person who can be directly or indirectly identified (i.e. with reference to other information available or obtainable) by reference to an identifier

5.2 **Identifiers** are personal information such as a name or ID number but can also include location data or online identifier or one or more factors such as physical, physiological, genetic, economic or social identity of that individual.

5.3 **Processing** means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with personal data;

5.4 **Data subject** means the living individual to whom the relevant personal data relates.

5.5 **Data controller** means the legal person i.e. the company or individual who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our employees.

5.6 **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

5.7 **Lawful basis/bases** is/are the legal reason(s) that permits the processing of personal data. Special categories of personal data are exempt from processing unless a further condition applies. Criminal records information can only be processed where the data is processed in an official capacity, or where there is a specific national legal that authorisation. Further information is provided in Appendix 1.

5.8 **'Legitimate interests'** is one of the six legal bases which can be relied upon where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.9 **Legitimate Interest Assessment** (LIA) is a type of 'light-touch' risk assessment that helps you ensure that a processing activity which seeks to rely upon legitimate interests as a legal basis is lawful. The assessment involves a careful consideration of the processing purpose, whether is necessary and whether it can be carried out in a way that does not override the data subject's interests.

5.10 **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes given by statement or by a clear affirmative action, that signifies agreement to the processing of their personal data.

5.11 **Sensitive personal data** is referred to in the GDPR as **special categories of personal data** and means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special categories of personal data do not include information about criminal offences and convictions but the GDPR requires similar safeguards for the processing of this type of data.

5.12 **Criminal records information** means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

5.13 **Data protection impact assessment** is a process to help identify and minimise the data protection risks associated with a project or specific processing activity.

5.14 **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6 ROLES & RESPONSIBILITIES

6.1 The Board is ultimately responsible for ensuring we conduct our data processing activities in line with data protection laws. The CEO and Executive Director are responsible for the supporting the implementation of the policy and ensuring it is effectively resourced.

6.2 Data Protection Officer (DPO)

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level on all matters relating to data protection and be given the required independence to perform their tasks which include:

6.2.1 Informing all staff, including the Board, Directors and Heads of Department about obligations under data protection laws and providing risk-based compliance advice;
6.2.2 Conducting internal audits to monitor compliance with the Policy and data protection laws;
6.2.3 Overseeing all internal data protection activities and maintaining records and other accountability documentation;
6.2.4 Raising awareness of data protection, working closely with Data Champions to ensure appropriate training is provided;
6.2.5 Advising on, and monitoring data protection impact assessments;
6.2.6 Cooperating with the ICO; and
6.2.7 Acting as the first point of contact for the ICO and for individuals whose data we process

6.3 Head of BGF

The Head of BGF is directly accountable for managing the privacy risks within BGF but may delegate specific responsibilities to an appropriately trained and competent staff member within BGF Responsibilities include:

6.3.1 Ensuring that all staff, volunteers and contractors who undertake processing activities understand their responsibilities under the Policy and complete the required training;

6.3.2 Responding to audit recommendations;

6.3.3 Ensuring the required documentation is completed and consulting with the DPO before undertaking any new processing activities;

6.3.4 Co-operating with the DPO as required to respond to requests from data subjects to assert their rights under data protection laws where the request relates solely or partially to processing activities carried out by the department;

6.3.5 Ensuring data protection impact assessments and other required assessments are completed as required in consultation with the DPO;

6.3.6 Where it is decided to not follow the advice given by the DPO, documenting the reason and recording any significant department privacy risks in the department risk register ensuring action to taken to control these risks;

6.3.7 Ensuring appropriate action is taken to address any repeated non-compliance with the Policy and operational guidance.

6.5 Data Owners

All personal data assets have a data owner who is responsible maintaining the asset in accordance with the data protection principles. Data Owners must ensure the asset is

6.5.1 Accurate and kept up to date and that any draft versions and duplicates are deleted;

6.5.2 Only accessible by those who need access to undertake their role;

6.5.3 Stored in the appropriate location;

6.5.4 Reviewed and deleted or archived in accordance with the applicable retention period.

6.6 All Staff, Volunteers and Contractors

Everyone is personally responsible for ensuring they conduct their own work activities in accordance with this policy and must:

6.6.1 Read and confirm understanding of the Policy;

6.6.2 Observe British Gymnastics Foundation Operational Guidance set out in Appendix 2.

6.6.3 Only carry out processing activities that are documented in the RoPA unless the Head of BGF or DPO has given prior authorisation;

6.6.4 Only access personal information that is required for the role;

6.6.5 Ensure personal information and actions relating to this data are recorded accurately in both manual and electronic records.

6.6.6 Report any actual or suspected personal data breaches or significant near misses without delay to the Head of BGF and DPO without delay.

6.7 Monitoring

This Policy will be regularly monitored to ensure it remains up-to-date. The following situations are also likely to evoke a review of the policy:

6.7.1 Any changes in the law or relevant guidance;

6.7.2 Following a significant civil or criminal case or enforcement action involving another organisation; and

6.7.3 A direct intervention by the ICO.

6.8 Reporting & Communications

6.8.1 The policy needs to be specifically communicated to the following individuals and groups:
- 6.8.1.1 All British Gymnastics Foundation Employees and Board members;
- 6.8.1.2 All British Gymnastics Foundation Volunteers who require access to personal information as part of their role;
- 6.8.1.3 All BGF Contractors who process personal data on our behalf.

6.8.2 The Head of BGF is responsible for communicating the policy and operational guidance to employees.

6.8.3 The responsibility for communicating the policy to other individuals rest with the relevant BGF staff member who is responsible for the work activity that the individual undertakes**.**

6.8.4 All individuals must sign to confirm that they have read the policy and understand how it relates to their individual responsibilities.

7 PROCEDURES

The DPO has overall responsibility for the ensuring the following procedures are applied in respect of all personal data we process working closely with the Head of BGF.

7.1 Lawful processing of personal data

7.1.1 Before commencing any processing activities for the first time, we will review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) set out in Appendix 1.

7.1.2 Except where the processing is based on consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

7.1.3 We will regularly review the processing activities we undertake to ensure that the identifies legal base or bases continue to be appropriate.

7.2 Legitimate interests

7.2.1 We recognise our additional responsibility for considering and protecting people's rights and interests where we are considering legitimate interests as the legal basis for a specific activity.

7.2.2 Before we rely upon this condition we will undertake a Legitimate interest assessment (LIA) to establish whether the processing is necessary and can be achieve in a balanced way that safeguards all individuals' interests, rights and freedoms.

7.2.3 If the LIA identifies a significant privacy impact, we will consider whether we also need to conduct a data protection impact assessment (DPIA);

7.2.4 We will keep the LIA under review, and repeat it if circumstances change.

7.3 Sensitive personal information

7.3.1 We will only process sensitive personal information if we have a lawful basis for doing so and one of the special conditions for processing sensitive personal information applies set out in Appendix 1.

7.3.2 Before processing any sensitive personal information, the Head of BGF must notify the DPO of the proposed processing and confirm whether the processing complies with the criteria noted above.

7.3.3 Sensitive personal information will not be processed unless the DPO has been consulted and the data subject has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

7.3.4 We will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

7.4

7.5 Data protection impact assessments (DPIA)

7.5.1 The purpose of a Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment to assess:

7.5.1.1 whether the processing is necessary and proportionate in relation to its purpose;
7.5.1.2 the risks to individuals; and
7.5.1.3 what measures can be put in place to address those risks and protect personal information.

7.5.2 Prior to undertaking any new processing determine the DPO must be consulted to determine whether a DPIA is required. We will undertake a DPIA where:

7.5.2.1 the proposed activity is likely to result in a high risk to the rights and freedoms of individuals; and/or
7.5.2.2 the processing involves the introduction of a new technology

7.6 Documentation and records

7.6.1 We will maintain a written record of processing activities (RoPA) as follows where the processing:

7.6.1.1 could result in a risk to the rights and freedoms of data subjects
7.6.1.2 is not occasional, or
7.6.1.3 involve special categories of personal data or criminal convictions and offences

7.6.2 We will also document any processing activities that involve sharing or disclosing personal information with a third-party.

7.6.3 Where personal information has been disclosed to a third-party, in a non-routine way the member of staff must consult with the DPO in advance and record the specific purpose for sharing on the individual's record.

7.6.4 The RoPA will include:

7.6.4.1 the purposes of the processing
7.6.4.2 a description of the categories of individuals and the categories of personal data
7.6.4.3 the categories of recipients of personal data

7.6.4.4 details of transfers of personal data to third countries or international organisations, including the transfer mechanism safeguards in place
7.6.4.5 retention schedules (where possible); and
7.6.4.6 a description (where possible) of the technical and organisational security measures that the employer has taken (appropriate to the level of risk) to ensure that personal data is kept secure

7.6.5 Where processing involves sensitive personal data, we will also document:
7.6.5.1 the lawful basis and additional condition we rely upon to process the data; and
7.6.5.2 whether the personal data is retained and erased in accordance with our retention schedule and if not, the reason why the retention schedule has not been applied.

7.7 Right to be informed

7.7.1 Individuals have the right to be informed about the collection and use of their personal data. We will provide this information in a concise, transparent, intelligible, easily accessible format using clear and plain language.

7.7.2 Where this information is provided by or relates to a child or someone who is known to be vulnerable for another reason, we will take steps to ensure this information is provided in a format that is appropriate to their age and ability to understand.

7.7.3 Our privacy policy provides the following information:
7.7.3.1 Our name and contact details of our organisation and the contact details of the DPO
7.7.3.2 The purposes of the processing.
7.7.3.3 The lawful basis for the processing.
7.7.3.4 The legitimate interests for the processing (if applicable).
7.7.3.5 The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
7.7.3.6 The recipients or categories of recipients of the personal data.
7.7.3.7 Details of any transfers of the personal data to any third countries or international organisations (if applicable).
7.7.3.8 The retention periods for the personal data.
7.7.3.9 The rights available to individuals in respect of the processing.
7.7.3.10 The right to withdraw consent (if applicable).
7.7.3.11 The right to lodge a complaint with a supervisory authority.
7.7.3.12 The source of the personal data (if the personal data is not obtained from the individual it relates to).
7.7.3.13 The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
7.7.3.14 The details of the existence of automated decision-making, including profiling (if applicable).

7.7.5 The BGF privacy policy is published on the BGF website at https://britishgymnasticsfoundation.org/privacy-statement/.

7.8 Other individual rights

7.8.1 Under data protection laws data subject have the following additional rights in relation to their own personal data:

7.8.1.1 the right of access to personal data and other supplementary information (this is known as a data subject access request, DSAR or SAR)

7.8.1.2 the right to rectification

7.8.1.3 the right to erasure (also known as the right to be forgotten)

7.8.1.4 the right to restrict processing

7.8.1.5 the right to data portability

7.8.1.6 the right to object

7.8.1.7 rights in relation to automated decision making and profiling (It is not expected that this right will impact upon as we do not process personal data by automated means).

7.8.3 Data subjects can exercise their rights in writing or verbally. There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

7.8.4 When a request is received, a response should be provided without undue delay and in any event within one month of receipt of the request. The time limit starts from the day after the request is received (irrespective of whether the day after is a working day or not) until the corresponding calendar date in the next month (or before if the next month has fewer days).

7.10 Requests for information by someone with parental responsibility for the data subject

7.10.1 Although individual rights under data protection laws rest with the data subject, as many of our beneficiaries are children, it is more likely that requests will come from someone who has parental responsibility. Where the request is simple or routine, the staff member should verify that the person requesting the information holds parental responsibility for the data subject. 7.10.2 Where information is being requested by an adult that we are unable to verify holds parental responsibility for the child, this information should not be provided without the specific authority of the data subject. If the data subject is under 13, this authority can be provided by the adult who is named on the account.

7.10.3 If the information being requested is sensitive or the staff member has any concerns relating to the provision of personal information, no information should be provided and the matter must be referred to the DPO for guidance. Where the data subject is over 13 and there is uncertainty about their wishes regarding the disclosure of sensitive information to a parent, the data subject's authority must be obtained prior in any information being shared.

7.11 Other third-party requests

7.11.1 Data protection laws do not prevent a third party making a subject access request on behalf of a data subject. Any request that is made by a third party other than someone with parental responsibility for the data subject should always be brought to the attention of the DPO.

7.11.2 It is the responsibility of the third party to demonstrate that they have the data subject's authority to act on their behalf. In responding, we will need to be satisfied that the third

party making the request has this authority and can request written authority from the data subject or a more general power of attorney where appropriate.

7.11.3 Where the DPO believes that the data subject has not understood fully what information will be disclosed to the third party who has made the request, the response will be sent directly to the data subject. The individual in question can then choose to share the information with the third party after having had a chance to review it first. Where a request is made by third party (e.g. a legal advisor), we will take steps to verify that the request was, in fact, instigated by the data subject and that the third party has the proper authority to act on their behalf.

7.12 Notification of a request

7.12.1 Any written or verbal request that is not simple of routine must be brought to the attention of the DPO without delay.

7.12.2 If a staff member receives a verbal request, even if they are uncertain as to the nature of the request, they should make a written record of all relevant details and explain that they will refer the matter to the DPO who will contact them.

7.12.3 If possible, the individual making the request should be encouraged, if they are willing, to confirm the request in writing to the DPO. If the individual is requesting a copy of information that we may hold about them, they should be advised that they can complete a subject access request contained in Appendix 3. If the individual wishes to object to a processing activity carried out in our legitimate interests, they should be encouraged to complete an objection to processing form provided in Appendix 4.

7.13 Next steps

7.13.1 The DPO is responsible for responding to all non-routine/simple requests from data subjects.

7.13.2 The DPO will assess the request and co-ordinate the response within the permitted time-period. All staff must support the DPO as required to ensure these timescales are achieved. The action taken will depend upon the nature of the request.

7.13.3 When we process a large quantity of information about an individual, the DPO may ask the individual to specify the information to which the request relates. We are not able to refuse a request on the basis that it relates to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

7.13.4 Where the DPO considers requests to be manifestly unfounded or excessive, we may:
a) charge a reasonable fee considering the administrative costs of providing the information (and the amount can be subject to limits); or
(b) refuse to respond.

7.13.5 Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the ICO without undue delay and at the latest within one month.

7.13.6 The DPO will consider the complexity and number of requests being made and may extend the permitted time periods by two further months where necessary. Where it has been determined that an extension is required, the data subject shall be informed within one month of receipt of the request and advised of the reasons for the delay.

7.13.7 The DPO will write to the individual to acknowledge the request and explain the legal situation and whether we will comply with the request.

7.13.8 The DPO will verify the identity of the person making the request, using reasonable means such as requesting specific identification documents, if we are not certain of their identity based on information that we already hold.

7.13.9 The DPO will inform the Head of BGF of any action that must be taken to comply with the request.

7.14 Searches

7.14.1 Where the requested information may be located in several filing and/or network systems and on mobile devices it is important to identify at the outset the type of information requested to enable a focused search.

7.14.2 Although the data subject is under no obligation to assist, the DPO may request that the scope of the request is narrowed to ease the searches to be undertaken. If we do not receive a useful clarification or any response at all, we will need to search all information we hold to comply with the request including:

7.14.2.1 All electronic systems (e.g. databases, networked and non-networked computers, servers, emails, CCTV and photography and video footage);

7.14.2.2 All company mobile phones and tablets

7.14.2.3 Manual/paper filing systems (but only if they are 'structured filing systems', on which see below); and

7.14.2.4 Any electronic data of data held in structured filing systems by our data processors.

7.14.3 All relevant systems will be searched using the individual's name, address, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different, and the DPO will agree the search parameters before commencing any search.

7.14.4 Information that is not part of a structured filing system, does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

7.15 Right of Access

7.15.1 Data protection laws provides individuals the right to obtain:

7.15.1.1 confirmation that their personal data is being processed;

7.15.1.2 access to their personal data; and

7.15.1.3 access to other supplementary information.

7.15.2 The individual is entitled to receive a description of the following:

7.15.2.1 the purposes for which we process the data;

7.15.2.2 the categories of personal data we process about them;

7.15.2.3 the recipients to whom we may disclose the data;

7.15.2.4 the duration for which the personal data may be stored;

7.15.2.5 the rights of the data subject under the data protection laws;

7.15.2.6 any information available regarding the source of the data if it was not collected from the data subject direct;

7.15.2.7 the right of the data subject to make a complaint to the supervisory authority for data protection;

7.15.2.8 the logic behind any automated decision we have taken about him or her (see below), the significance and consequences of this automated processing.

7.15.3 We must provide the information constituting the individual's personal data which is within the scope of their request. We must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically we can, unless the data subject specifies otherwise, also provide the information in electronic form.

7.16 Redactions

7.16.1 Where we are providing information to an individual where they have made a subject access request, they are only entitled to their personal data. Although we may provide non-personal information on a discretionary basis, they are not entitled to see information which relates to other individuals and such information will usually be redacted unless it is already known by the data subject.

7.16.2 Sometimes information that is determined to be personal data about the person making the request might also include information that identifies or is the personal data of another person e.g. a letter of complaint. In some cases, it is not possible to redact the information about the other person but the information can be disclosed if the other person has consented.

7.16.3 Where the other person has not consented, the DPO in consultation with the Head of BGF will consider whether it would be reasonable in the circumstances to disclose this information to the person making the request.

7.16.4 In making this decision, we will consider:

7.16.4.1 Whether asking for consent might reveal the identity of the individual making the request and if we owe that person a duty of confidentiality;

7.16.4.2 What steps we have taken to obtain the consent of the other person;

7.16.4.3 Any specific reason why the other person has refused their consent;

7.16.4.4 Any reason why the other person's consent cannot be obtained e.g. because they are incapable of giving it due to illness or incapacity;

7.16.4.5 If the other person is the source of the information;

7.16.4.6 If there is an imbalance of power or authority between the person making the request and the other person and if the data may be used in a way that is to the other person's disadvantage;

7.16.4.7 Whether the information is generally known by the individual making the request; and

7.16.4.8 Where the person making the request has a legitimate interest in the disclosure of the other person's information which they have made known to us.

7.16.5 If we decide that the other person's information should be withheld, we still have to provide as much information as we can without compromising the other person's identity. Therefore, redactions should be limited to those specifically required to protect the other person's identity.

7.16.6 The DPO will keep a record of what has been redacted and the reason for doing so.

7.17 Exemptions to the right of subject access

7.17.1 There are certain circumstances where an exemption to providing personal data in response to a subject access request may apply.

7.17.2 All following exemptions will be considered and applied on a case by case basis after a careful consideration of all the facts.

- 7.17.2.1 Crime detection and prevention
- 7.17.2.2 Confidential references
- 7.17.2.3 Legal professional privilege
- 7.17.2.4 Management forecasting
- 7.17.2.5 Company negotiations

7.17.3 The DPO may seek external legal advice as necessary in relation to whether an exemption can be applied in a particular case.

7.18 Right to Erasure

7.18.1 Data subjects have the right to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

7.18.2 The right to erasure is not an absolute right and applies only as follows:

- 7.18.2.1 where personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- 7.18.2.2 when the data subject withdraws consent (but only to the extent that consent is the only basis for processing their personal data);
- 7.18.2.3 where the data subject objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing;
- 7.18.2.4 where the personal data was unlawfully processed;
- 7.18.2.5 where the personal data has to be erased in order to comply with a legal obligation; and
- 7.18.2.6 where the personal data is processed in relation to the offer of information society services to a child.

7.18.3 There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request if we require the personal information:

- 7.18.3.1 to exercise the right of freedom of expression and information;
- 7.18.3.2 to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- 7.18.3.3 for public health purposes in the public interest;
- 7.18.3.4 archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- 7.18.3.5 the exercise or defence of legal claims.

7.18.4 If we have disclosed the personal data to be erased to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

7.19 Right to rectification

7.19.1 An individual has the right to ask us to:

7.19.1.1 correct inaccurate personal data;
7.19.1.2 complete information if it is incomplete; and
7.19.1.3 delete personal data which is irrelevant or no long required for our purposes.

7.19.2 Where information has been provided to a third-party, we must inform them of the rectification request where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

7.19.3 The DPO will assess whether the information that the data subject is asking to be deleted is factually correct and whether there is justification for retaining it, i.e. it is relevant to the lawful purpose for which we are holding it and whether we can continue to retain the information on that basis.

7.19.4 The DPO will explain to the data subject if we are not taking any action in response to a request for rectification and inform them of their right to complain to the ICO and to seek a remedy from the Courts.

7.20 Right to Restrict Processing

7.20.1 An individual is entitled to require us to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We can retain just enough information about the individual to ensure that the restriction is respected in future.

7.20.2 We are required to restrict the processing of personal data in the following circumstances:

7.20.2.1 Where a data subject challenges the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data;
7.20.2.2 Where a data subject has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual;
7.20.2.3 When processing is unlawful and the individual opposes erasure and requests restriction instead; and
7.20.2.4 If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

7.20.3 This right to restrict processing does not apply if the individual has entered into a contract with us and the processing is necessary for the fulfilment of that contract.

7.20.4 Where a request to restrict processing is received, the DPO will implement restrictions where the right is applicable. The DPO will then assess the matter, where appropriate in consultation with the Head of BGF and will inform the data subject of the action taken and specifically advise when we decide to lift a restriction on processing e.g. if an individual contested our right to process their personal data on legitimate interest grounds and we subsequently found that there was compelling justification to continue to process the individual's data.

7.20.5 If we have disclosed the restricted personal data to third parties, the DPO will inform them if we have agreed to erasure any personal data, unless it is impossible or involves disproportionate effort to do so.

7.21 The Right to Data Portability

7.21.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

7.21.2 The right to data portability only applies:

7.21.2.1 to personal data an individual has provided to a data controller;
7.21.2.2 where the processing is based on the individual's consent or for the performance of a contract; and
7.21.2.3 when processing is carried out by automated means.

7.21.3 We must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. The information must be provided free of charge.

7.21.4 If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

7.21.5 The DPO will review and co-ordinate any requests relating to data portability.

7.22 Right to Object

7.22.1 Individuals have the right to object to:

7.22.1.1 processing based on legitimate interests;
7.22.1.2 the performance of a task in the public interest/exercise of official authority (including profiling);
7.22.1.3 direct marketing (including profiling); and
7.22.1.4 processing for purposes of scientific/historical research and statistics.

7.22.2 Where a data subject objects, the DPO, in consultation with the Head of BGF will consider the individual grounds for objection relating to his or her particular situation.

7.22.3 We will stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

7.22.4 Any objection relating to process personal data for direct marketing purposes is absolute and we must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse. We will maintain a suppression list so that we can comply with any objections received.

7.23 Deleting personal data in the normal course

7.23.1 We are only required to supply information in response to an exercise of individual rights that was processed at the date of that request. However, we are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

7.23.2 In no other circumstance will we amend or delete data because we do not want to supply it or because of the exercise of a right.

7.24 Information security

7.24.1 We recognise our responsibility to implement appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

7.24.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

7.24.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

7.24.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

7.24.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

7.25 Data Processors

7.25.1 We will only use external organisations or individuals to carry out processing activities on our behalf, where there is a written contract in place that ensures the organisation or individual:

7.25.1.1 Only acts in accordance with our written instructions

7.25.1.2 Is subject to a duty of confidence;

7.25.1.3 Implements appropriate measures to ensure the security of processing;

7.25.1.4 Does not engage any sub-processor unless we have given our prior consent and the sub-processor is also subject to these requirements;

7.25.1.5 Assists us in providing subject access and allowing individuals to exercise their rights in relation to data protection;

7.25.1.6 Assist us in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

7.25.1.7 Deletes or returns all personal information to the Company as requested at the end of the contract; and

7.25.1.8 Submit to audits and inspections and agrees to provide each other with whatever information required to ensure we are both meeting our data protection obligations; and

7.25.1.9 Advise us immediately if asked to do something infringing data protection law.

7.25.2 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

7.26 Storage and retention of personal information

7.26.1 Personal information (and sensitive personal information) will be kept securely in accordance with our data security statement.

7.26.2 We will maintain a retention schedule that sets out the specific periods for which we will retain each type of personal data. The retention periods will take account of any statutory requirements as well as other lawful reason why we need to retain the information. and to securely disposing of any personal information where we no longer have a lawful reason to hold it. provide information

7.26.3 Personal information (and sensitive personal information) will not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

7.26.4 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

7.26.5 All information will be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

7.26.6 Hard copy and electronically-held documents and information will be disposed of by shredding or deleted at the end of the retention period.

7.27 International transfers

7.27.1 We may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) where it is permitted under data protection laws as follows:

7.27.1.1 Where the country, territory or organisation is designated as having an adequate level of protection; or

7.27.1.2 The organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct; or

7.27.1.3 If it is absolutely necessary for the performance of a contract or with the explicit consent of the data subject.

7.28 Data breaches

7.28.1 We have established a Data Breach Team who are responsible for responding to any suspected or actual personal data breaches.

7.28.2 The Data Breach Team (DBT) is made up of the following:

7.28.2.1.1 Data Protection Officer

7.28.2.1.2 Head of BGF

7.28.2.1.3 Trustee responsible for Risk 23 (breaches of GDPR legislation)

7.28.4 All staff, volunteers and contractors are responsible for reporting any suspected or actual data breaches without delay to the Head of BGF and the DPO who must ensure the DBT are immediately notified.

7.28.5 The person who discovers/receives a report of a serious security incident must inform the DPO and the Head of BGF without delay even if the incident occurs outside office hours.

7.28.6 Employees or others acting on behalf of British Gymnastics Foundation must never attempt to conceal or deal with the incident beyond ensuring it is reported without delay.

7.28.7 The personal data breach will then be managed in accordance with the plan set out in Appendix 5.

7.28.8 We will report to the Information Commissioner's Office without undue delay and within 72 hours of becoming aware of it any breach that results in a risk to the rights and freedoms of individuals. We will also notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms.

7.29 Training

7.29.1 We will ensure that all staff, volunteers and contractors receive appropriate training regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

7.30 Consequences of failing to comply

7.30.1 Failure to adhere to this policy could result in individuals being criminally liable for deliberate unlawful disclosure of personal information. This may result in criminal prosecution and/or disciplinary action. We take compliance with this policy very seriously. Failure to comply with the policy:

7.30.1.1 puts at risk the individuals whose personal information is being processed; and

7.30.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

7.30.1.3 may, in some circumstances, amount to a criminal offence by the individual.

7.30.2 We will ensure that all staff, volunteers and contractors comply with this policy, operational guidance and procedures as far as they are relevant to their individual role and responsibilities and will use the provisions contained in terms and conditions of employment, contracts for service and specific data processing clauses to carry out any investigation and where appropriate take disciplinary action where there is a concern that any individual may have acted in a way that does not comply our policy and/or data protection law. Where it is determined, in accordance with the relevant disciplinary procedures that an individual has failed to comply, this could lead dismissal or termination of a contract or voluntary position.

8 INTERDEPENDENCIES/ RELATED POLICIES

8.1 Database Retention Policy

8.2 Use of Criminal Records Checks Policy

Appendix 1

1 Lawful Conditions for Processing Personal Data

The following lawful bases for processing are set out in Article 6 of the GDPR.
At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

2 Conditions for processing special category data

These conditions are listed in Article 9(2) of the GDPR

(a) 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;
(b) 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;
(c) 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;
(d) 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;
(e) processing relates to personal data which are **manifestly made public by the data subject**;
(f) processing is **necessary for the establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;
(g) 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;
(h) 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;

(i) 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;

(j) 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.

3 Criminal Convictions

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that if you are processing personal criminal offence data, you will also need to comply with Article 10.

Article 10 says:
"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

This means that the controller must either be processing the data in an official capacity, or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill.

Even if a condition for processing offence data, organisations can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.

Appendix 2: BRITISH GYMNASTICS OPERATIONAL GUIDANCE FOR PROCESSING PERSONAL DATA

This guidance applies to you if you are a British Gymnastics employee (including employees seconded to BGF). It also applies to you if you undertake a voluntary role and have access to personal information as part of that role. It also applies to you if you are a contractor for BGF..

While you have responsibilities in respect of any personal information you handle that relates to another person, you also have a responsibility to keep your own personal information up to date.

You must only access the personal information that you have authority to access, and only use it for approved purposes. You must comply with the following guidance at all times in respect of its use:

1 Security when working in a shared or public space

1.1 Ensure personal data is not seen or accessed by unauthorised individuals.
1.2 If working at Lilleshall or another shared office space, do not allow anyone into the premises unless you are certain that they have authority to be there and ensure you do not leave visitors unsupervised.
1.3 Never share or write down computer or telephone passwords and always lock your computer screen or mobile if leaving the device unattended.
1.4 If using a shared printer use private print if available when printing documents that contain personal data
1.5 Take care not to leave documents containing personal data lying around or on the printer, photocopier or scanner or pick up someone else's documents
1.6 Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office
1.7 When in a public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.

2 General Security

2.1 Avoid printing or downloading documents unless it is absolutely necessary.
2.2 Always ensure personal information is stored securely in a locked filing cabinet or a lockable bag if being transported.
2.3 When travelling by car, papers must always be stored in the boot of the car and must not be left in the car overnight.
2.4 Ensure all confidential waste and paperwork containing personal data is disposed of securely by shredding.
2.5 Never use removable storage media to store personal data unless the personal data on the media is encrypted or the USB stick itself is encrypted.
2.6 Do not remove personal information on electronic devices from your office premises unless appropriate security measures are place (such as pseudonymisation, encryption or password protection) to secure the information and the device;
2.7 Do not store personal information on personal devices that are used for work purposes unless you have the authority of the Head of IT. This will usually only be provided where your personal device is encrypted.
2.8 Ensure you have a strong password on any IT devices and ensure it is changed at least every six months;
2.9 Do not disclose your unique logins and passwords to anyone except when required by authorised IT staff;

2.10 Do use password to protect documents and databases containing sensitive personal data.

3 Telephone communications

Personal information should only be disclosed over the telephone to a third-party where the following guidelines have been applied:

3.1 The identity of the other party has been verified. No information should be released to a third party without confirming that the person requesting the information has the authority of the data subject;

3.2 Where sensitive information is being requested by a third party representing another organisation; request contact details and call the person back via the main number for their organisation, asking for the person by name, and only provide the information to the person who requested it.

3.3 Do not leave any confidential information on voicemail or answering machines as it may be accessible by others. Remember that even confirming an individual is an employee or member of British Gymnastics would be considered personal information.

3.4 When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

3.5 Never act on instructions from someone unless you are absolutely certain of their identity. This is particularly relevant where instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

4 Electronic communication

In view of the potential impact on individuals if their personal data is lost or misdirected, the following guidelines apply to email communications particularly where personal information is provided in bulk (i.e. multiple individual records) or where the information is of a sensitive nature.

4.1 Sensitive personal information should only be sent via the internal British Gymnastics email and should never be transmit using a fax machines or via text messaging, messaging services or social media.

4.2 Personal data should not be stored or shared using free cloud storage or sharing apps. Third party services must only be used where we have a data processing agreement in place;

4.3 Where it is absolutely necessary to send sensitive information externally, it must be encrypted/password protected. The exception for this is where the data subject has confirmed (in writing) that they want to receive their personal information without encryption.

4.4 Care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate interest.

4.5 If information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending.

4.6 Never send sensitive personal information to a group or shared email address where there is any uncertainty about security.

4.7 Careful consider whether it is appropriate to the use of e-mail distribution lists and always use the blind carbon copy (bcc) option when sending out e-mails to multiple recipients unless it is absolutely clear that every recipient of the email would already have each other's email address or would expect for their personal data to be shared in this way.

4.8 If you are expressing an opinion about an individual, always substantiated your opinions. Remember that individuals have a right of access to this information.

5 Sharing personal data with third parties

5.1 Only share information with other individuals if they have appropriate authority to access it or you have the specific authority to do so from the Head of Department or DPO;
5.2 Always contact Head of Department of DPO if you are concerned or suspect that someone without authority has had access to the personal data you hold;
5.3 Do not discuss any confidential personal information that you have been provided or come aware of during your work or activities for British Gymnastics Foundation in the presence of anyone who does not have a legitimate reason to know;
5.4 Verify that the person who has requested personal data is authorised to receive it prior to disclosure;
5.5 Do not disclosure personal information about British Gymnastics staff, volunteers or members to any other individuals including, unauthorised colleagues, family or friends; and
5.6 Ensure personal data is anonymised in reports or audits unless you have specific authority from the Head of Department.

6 Recruitment & Selection (only employs to those involved in recruitment)

6.1 Never ask questions relating to sensitive personal information during the recruitment and selection process except where this is permitted by law and/or there is a legal obligation to do so.
6.2 Do not record any sensitive personal information that is disclosed during interview.
6.3 Ensure any sensitive personal information disclosed by an applicant on a CV or application form is immediately deleted or redacted.
6.4 Ensure any completed equal opportunities monitoring forms are kept separate to individual application forms and not shared with the person shortlisting, interviewing or making the recruitment decision.
6.5 Do not ask health questions until an offer has been accepted except information relating to a disability where it is provided for the purpose of providing reasonable adjustments at interview.

Appendix 3 - Objection to data processing under legitimate interests

There are some processing activities that we undertake because they are in our legitimate interests (or those of a third party). These activities are outlined in our privacy notices. You have a right to object to such processing. In some cases, if you object we will cease the processing your personal data for the purpose to which you object. However, in other cases, we will first need to undertake an assessment to determine whether your objection to a specific purpose is sufficient to override the legitimate interest in continuing to process the data for that purpose. Where appropriate, we will consider whether the processing activities can be refined or limited or additional safeguards put in place.

You can raise an objection by completing this form. We will consider and respond to all objections within 21 days. Please bear in mind that in some cases, objections to processing may affect our ability to provide services intended for your benefit.

DATA SUBJECT:

_____**DOB**_____

CONTACT DETAILS:

_____

_____

DETAILS OF THE PROCESSING TO WHICH YOU OBJECT _____

_____

REASON FOR OBJECTION (Please outline any damage or distress that would be caused to the data subject by this data processing)

_____

_____

_____

ACTION REQUESTED (please explain what you want British Gymnastics Foundation to do)

_____

_____

_____

SIGNED:

_____

(By data subject if over 13 years of age)

SIGNED

_____

(and/or by Parent If under 16 years of age)

Please return your completed form to [insert name and email address of contact at British Gymnastics Foundation] at least four weeks before the date of the event in question. Objections will be considered and a response provided within 21 calendar days of receipt of the objection.

Appendix 4: SUBJECT ACCESS REQUEST (SAR) FORM

There is no requirement to complete this form but the information provided will help British Gymnastics Foundation to respond to your request in the most efficient manner.

The right of access applies to the data subject who can authorise another person to act on their behalf. Without the authority of the data subject, we will not provide this information to a third-party unless the data subject is unable to make this request independently due to their age or mental capacity.

Data Subject Name:	
Address or email	
Membership No. (if applicable)	
Telephone Number:	
DoB:	

Required information:

Authority

If you are acting on behalf of the person to whom the data relates, please state your relationship with the afore mentioned individual and include your contact details if they are different from the above.

Please return this form to the Data Protection Officer at British Gymnastics Foundation, Lilleshall NSC, Newport, Shropshire, TF10 9AT. In most cases, we will respond without delay and at the latest within one month of receipt of the request. We may have to extend the time allowed by a further two months where requests are complex or numerous but will inform you if this is the case. We will also contact you if we require additional information to verify your identity.

Appendix 5: BRITISH GYMNASTICS FOUNDATION DATA PROTECTION BREACH PLAN

1 Responsibilities

1.1 The DPO has overall responsibility for the Data Protection Breach Plan. British Gymnastics has established a Data Breach Team (DBT) whose function is to respond to any actual or suspected Personal Data Breaches. The DPO must ensure the DBT take a standardised management approach in the event of a security incident and ensure details of any such incident are recorded and reported in line with our legal obligations under Data Protection Laws.

1.2 This plan aims to ensure that breaches or potential breaches are dealt with speedily and efficiently and ensure damage is kept to a minimum and lessons are learnt.

1.3 A personal data breach can occur for a range of reasons. Some examples include:

1.3.1 Loss or theft of IT equipment or information e.g. laptop or paper file
1.3.2 Disclosing personal information to someone not authorised to have it.
1.3.3 Inappropriate access controls allowing unauthorised use
1.3.4 Breach of physical building security.
1.3.5 Uploading personal information to a website in error.
1.3.6 Equipment failure.
1.3.7 Human error e.g. sending an email to the wrong recipient or not sending a group email by blind copy
1.3.8 Unforeseen circumstances such as a fire or flood
1.3.9 Hacking, phishing and other 'blagging' attacks where information is obtained by deceiving whoever holds it

1.4 All staff are required to report any actual or suspected personal data breaches to Head of BGF and the DPO.

1.5 The DPO is responsible for ensuring that the remaining members of the Data Breach Team (DBT) are notified and action is taken in accordance with the plan set out below.

1.6 As soon as the Head of BGFis made aware of an actual or suspected breach, he/she must liaise with their team member without delay to accurately record details of the incident and ensure the following information is provided to the DBT: -

1.6.1 Date and time of security incident / period of time occurred.
1.6.2 Date and time security incident detected.
1.6.3 Who reported the security incident?
1.6.4 Description of the security incident.
1.6.5 Approximate number of data subjects affected.
1.6.6 Details of any ICT systems or third-party systems involved.
1.6.7 Details of any action taken to minimise / mitigate the effect on data subjects.
1.6.8 Details of anyone who is aware of the security incident.
1.6.9 Brief details of any supporting material which either confirms the incident or is related to the incident.
1.6.10 Details of any other organisations, contractors or volunteers involved.

1.7 Details of data protection incidents can be very sensitive and any sensitive information must be handled with discretion and only disclosed to those who need to know the details.

1.8 Any staff member who received a report of a breach or enquiries in connection with a breach should attempt to obtain the name and contact details of the individual and pass the information to the DBT.

2 DATA BREACH MANAGEMENT

2.1 The DBT will respond to all suspected breaches as follows: -

a) Containment and recovery.
b) Assessment of ongoing risk.
c) Notification of breach.
d) Evaluation and response.

3 CONTAINMENT AND RECOVERY

3.1 Containment and recovery involves limiting the scope and impact of the data breach, and stemming it as quickly as possible.

3.2 The following steps must be taken as soon as possible:

3.2.1 The DBT must inform the Trustees and British Gymnastics Foundation insurers where appropriate.

3.2.2 The DBT must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred or where there is a risk that illegal activity might occur in the future as a result of the breach. The police may also assist in locating stolen hardware or data.

3.3 Depending on the nature of the breach, the DBT will notify our insurers

3.4 The DBT will identify which of the following three categories the incident fits: -
a) An actual or suspected data breach;
b) A serious IT security incident that is not a data breach;
c) Another type of serious security incident that puts personal information at risk but is not a data breach.

3.5 The DBT will agree who will lead the Investigation. The agreed person will, without delay, take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include: -

3.5.1 Attempting to recover any lost equipment or personal information.
3.5.2 Shutting down an IT system.
3.5.3 Contacting key departments/employees so that they are prepared for any potentially inappropriate enquiries about the affected data subjects.
3.5.4 Using back-up data to restore lost or damaged or stolen information.
3.5.5 If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

3.6 The DBT should consult with BG's Head of Marketing & Communications:

3.6.1 To agree any internal communications.

3.6.2 To ensure they are prepared to handle any press enquiries or to make any press releases.

4 ASSESSMENT OF ONGOING RISK / INVESTIGATION

4.1 In most cases the next stage would be for the person nominated by the DBT to fully investigate the breach to ascertain whose information was involved in the breach, the potential effect on the data subjects and what further steps are required to remedy the situation.

4.2 The investigation should consider: -

4.2.1 The type of information;
4.2.2 Its sensitivity;
4.2.3 The number of individuals affected by the breach;
4.2.4 What group of people have been affected (staff, members, children etc.)
4.2.5 What protections are in place (e.g. encryption);
4.2.6 What happened to the information;
4.2.7 Whether the information could be put to any illegal or inappropriate use.
4.2.8 What could the information tell a third party about the individual;
4.2.9 Whether there are wider consequences to the breach.

4.3 A clear record should be made of the nature of the breach and the actions taken to mitigate it. The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered and reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved

5 NOTIFICATION

5.1 Certain individuals and organisations may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place.

5.2 The data breach team will consider whether to notify the ICO and the affected data subjects.

6 Notifying the ICO

6.1 The data breach team will notify the ICO when a personal data breach has occurred, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

6.2 Where ICO notification is required, this shall be done by the DPO without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

6.3 If the data breach team is uncertain whether to report, the presumption should be to report.

6.4 In considering whether a report is required the data breach team will take account of the following factors:

6.4.1 The potential harm to the rights and freedoms of data subjects
6.4.2 The volume of the personal data
6.4.3 The sensitivity of the personal data

6.5 If a decision is taken not to report, a record will be maintained of the reasons for the decision.

7 Notifying data subjects

7.1 Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data breach team will notify the affected data subject(s) without undue delay, including:

7.1.1 the name and contact details of the data protection officer or other contact point where more information can be obtained;
7.1.2 the likely consequences of the personal data breach;
7.1.3 the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

7.2 When determining whether and how to notify data subjects of the breach, DBT will co-operate closely with the ICO and other relevant authorities, e.g. the police and will take account of the following factors:

7.2.1 Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.
7.2.2 Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.
7.2.3 Whether it would involve disproportionate effort to notify the data subject(s).
7.2.4 Whether there are any legal or contractual requirements to notify the data subject?

8 Notifying the police

8.1 The data breach team will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against [or by a representative of] [insert organisation's name], the data breach team will notify the police and/or relevant law enforcement authorities.

9 MONITORING AND REVIEW

9.1 Once the personal data breach has been dealt with, in accordance with this plan, the DBT will conduct a post-breach review and:

9.1.1 Establish what security measures were in place when the breach occurred
9.1.2 Assess whether technical or organisational measures can be implemented to prevent the breach happening again
9.1.3 Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
9.1.4 Consider whether it is necessary to conduct a data protection risk assessment
9.1.5 Update British Gymnastics data protection risk register

9.2 If a systemic or on-going problem is identified, then an action plan must be drawn up to ensure this is rectified.

9.3 The DPO will keep detailed record of all reported breaches and make these records available to the Board.

9.4 This plan will be reviewed annually, after a breach and after legislative changes, new case law or new guidance.