GBS Data Breach Policy

Version	Date Reviewed	By
1.0	21/06/2019	CEO

Contents

Definitions 3

Introduction 4

Aims 4

Scope 4

Types of Breach 5

Reporting an Incident 6

Containment and Recovery 6

Investigation 6

Notification 7

Evaluation and Response 8

Record Keeping 8

Definitions

“DPA”	means the Data Protection Act 2018;
“GBS”	means GB Snowsport;
“GBS CEO”	means the Chief Executive of GBS;
“GBS Website”	means the official GBS website, https://www.gbsnowsport.com/;
“GDPR”	means the General Data Protection Regulation (EU) 2016/679;

1. Introduction

1.1. This Document contains the GB Snowsport (GBS) Data Breach Policy. GBS is required under data protection legislation such as the Data Protection Act 2018 ("DPA") and the General Data Protection Regulation (EU) 2016/679 ("GDPR") to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

1.2. This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing any data breach and information security incidents across GBS.

Aims

1.3. To comply with relevant data protection law, such as the Data Protection Act 2018 ("DPA") and the General Data Protection Regulation (EU) 2016/679 ("GDPR") and to follow good practice.

1.4. To protect the rights of GBS staff, athletes, volunteers, and anyone working on behalf of GBS.

1.5. To contain any breaches, to minimise the risk associated with the breach, and consider what remedial action is necessary to secure personal data and prevent further breaches.

Scope

1.6. This Policy is to be followed by all GBS staff, athletes, and volunteers, and anyone working on behalf of GBS.

1.7. This Policy applies to all data that GBS may hold relating to identifiable individuals even if that information technically falls outside of the DPA or GDPR. This may include details such as names of individuals, postal and email addresses, telephone numbers, and GBS contacts.

1.8. Failure to comply with this Policy will lead to disciplinary action in line with the GBS Disciplinary Policy. If your conduct is unlawful or illegal you may be personally liable.

1.9. GBS recognises its legal obligations under both the GDPR and the DPA (which is the UK's implementation of the GDPR) and will abide by its requirements, as well as any equivalent legislation (as amended) in any UK jurisdiction, Jersey, Guernsey or the Isle of Man and any later amendments to such legislation or subsequent equality related legislation that may be relevant to GBS.

1.10. This Code is designed to be read in conjunction with the GBS Data Protection Policy.

2. Types of Breach

2.1. For the purposes of this Policy, data security breaches include both confirmed and suspected incidents.

2.2. An "incident" in the context of this Policy is an event which may compromise the confidentiality, integrity, or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to GBS' information assets and/or reputation.

2.3. An incident includes, but is not restricted to the following:

2.3.1. Loss or theft of confidential or special category data, or equipment on which such data is stored (e.g. loss of a laptop, memory stick, iPad/Tablet, or paper record;

2.3.2. Equipment theft or failure;

2.3.3. Unauthorised use, access, or modification of data or information systems;

2.3.4. Attempts (failed or successful) to gain unauthorised access to information or IT systems;

2.3.5. Unauthorised disclosure of special category and confidential data;

2.3.6. Website defacement;

2.3.7. Hacking attack;

2.3.8. Unforeseen circumstances such as a fire or flood;

2.3.9. Human error; and

2.3.10. Blagging offences where information is obtained by deceiving the organisation who holds it.

3. Reporting an Incident

3.1. Any individual who accesses, uses or manages GBS' data is responsible for reporting the data breach and information security incidents immediately to the CEO. This will trigger a report to GBS' appointed Data Protection Officer (DPO). In the event the DPO is unavailable the GBS IT lead will be informed.

3.2. If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. GBS has 72 hours to report a breach to the Information Commissioner's Office (ICO) if it is decided under Clause 6 that the breach needs to be reported.

3.3. The report will include full and accurate details of the incident, when the breach occurred, details of the person reporting the breach, whether the breach relates to people, the nature of the information, and how many people are involved. A Data Breach Report Form should be completed as part of the reporting process.

4. Containment and Recovery

4.1. The DPO will firstly determine if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effect of the breach.

4.2. An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach.

4.3. The Lead Investigation Officer (LIO) will establish who may need to be notified as part of the initial containment and will inform the police, if appropriate.

4.4. The LIO, in liaison with the relevant officers will determine a suitable course of action to be taken to ensure a resolution to the incident.

5. Investigation

5.1. An investigation will be undertaken by the LIO immediately and where possible within 24 hours of the breach being discovered or reported.

5.2. The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse effects for individuals, how serious or substantial those are and how likely they are to occur.

5.3. The investigation will need to take into account the following:

5.3.1. the type of data involved;

5.3.2. its sensitivity;

5.3.3. the protection in place (e.g. encryption);

5.3.4. what has happened to the data, if it has been lost or stolen;

5.3.5. whether the data could be put to illegal or inappropriate use;

5.3.6. who the individuals are, the number affected and the potential effects on those data subjects; and

5.3.7. whether there are wider consequences to the breach.

6. Notification

6.1. The LIO and/or the DPO, in consultation with the CEO will determine whether the breach needs to be reported to the ICO.

6.2. Every incident will be assessed on a case by case basis against the following considerations:

6.2.1. whether there are any legal or contractual notification requirements;

6.2.2. whether notification would assist the individual affected – could they act on information to mitigate the risks;

6.2.3. whether notification would help prevent the unauthorised or unlawful use of personal data;

6.2.4. would notification help GBS meet its obligations under the principle; and

6.2.5. whether this breach constitutes a high risk to individuals and therefore needs to be reported to the ICO.

6.3. Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact GBS for further information or to ask questions about what has occurred.

6.4. The LIO and/or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. 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.

6.5. The LIO and/or DPO will consider whether any press release may be required.

6.6. All actions will be recorded by the LIO and DPO.

7. Evaluation and Response

7.1. Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies, or procedures should be undertaken.

7.2. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

7.3. The review will consider:

7.3.1. where and how the personal data is held and where it is stored;

7.3.2. where the biggest risks lie, and will identify any further potential weak points within its existing measures;

7.3.3. whether methods of transmission are secure - sharing the minimum amount of data necessary;

7.3.4. identifying weak points within existing security measures;

7.3.5. staff awareness; and

7.3.6. implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8. Record Keeping

8.1. The GDPR requires us to keep full and accurate records of personal data breaches that are maintained, setting out the facts surrounding the breach, its effects, and any action taken after the evaluation.