DATA PROTECTION GDPR

Snowbility Limited Data Protection Policy No. ZA184284

Awareness

All Snowbility Limited's ("Snowbility") staff, as part of their induction, must read and sign the company's NDA agreement that includes the Data Protection Policy.

Snowbility's database system (Zoho)

What is personal data or Personally Identifiable Information (PII)?

Any information relating to an identified or identifiable natural person. The identifiers are classified into two types: direct (e.g., name, email, phone number, etc.) and indirect (e.g., date of birth, gender, etc.).

What are the key changes from the previous Regulations?

New and enhanced rights for data subjects - This law gives an individual the right to exercise complete authority over their personal data. Some of the rights highlighted in the Regulations are:

- **Explicit consent** - Individuals must be informed about how their personal data will be processed. Organisations must make it as easy for individuals to withdraw their consent, as it is to grant it.
- **Right to access** - At any point in time, the individual an ask the organisation what personal data is being stored or retained about him/her.
- **Right to be** forgotten - **The** individual can request the organisation to remove their personal information from the oganisation's systems.
- **Data** portability - **The** organisation must be able to provide individuals with a copy of their personal data in machine readable format. If possible, they must be able to transfer the data to another organisation.
- **Obligations of the processors** - GDPR has raised the bar for the responsibilities and liabilities of data processors as well. Processors must be able to demonstrate compliance with the GDPR and they must follow the data controller's instructions.
- **Data Protection Officer** - Organisations may need to appoint a staff member or external service provider who is responsible for overseeing GDPR, general privacy management compliance and data protection practices.
- **Privacy Impact Assessments (PIA)** - Organisations must conduct privacy impact assessments of their large-scale data processing to minimize the risks and identify measures to mitigate them.
- **Breach notification** - Controllers must notify the stakeholders (the supervisory authority, and where applicable, the individuals) within 72 hours of becoming aware of a breach.

Does the GDPR require EU personal data to stay in the EU?

No, the GDPR does not require EU personal data to stay in the EU, nor does it place any new restrictions on transfers of personal data outside the EU. Our data processing addendum, which references the European Commission's model clauses, will continue to help our customers facilitate transfers of EU personal data outside of the EU.

Where is my data located?

The data of zoho.com customers will reside in the US data centres and that of zoho.eu will reside in the EU data centres.

Information that Snowbility holds

Snowbility documents the personal data it holds, where the data came from and who the company shares it with.

Snowbility maintains records of the processing activity:

- All data Snowbility holds is provided to the company by the parents or carers of its students or directly by a student where they are over 18 years old. This data is provided so that Snowbility can access its coaching process and understanding of a student's needs.
- The form Snowbility use is called an initial assessment form and is held in such a way that it cannot be altered by a staff member.
- Snowbility also holds information on the snow sports activity undertaken by the student and this data is put into the company's ski pass by the instructor after a lesson.

Communicating confidential information

Snowbility has a Privacy Policy which is on its website www.snowbility.co.uk.

Individual's rights

Where Snowbility receives a request to delete personal data, the company complies immediately with this. There are also relevant fields on Snowbility's database that the company can tick if an individual has requested they do not want to receive any form of correspondence from Snowbility.

Individual access requests

The procedure of how Snowbility handles individual requests is actioned by emailing either Richard Fetherston, Kathryn Morris or Lesley McDonald.

Lawful basis for processing personal data

Snowbility only processes data related to its main activity which is snow sports coaching for additional needs students.

Consent

All data Snowbility holds is freely given to the company by parents and carers related to a student who has signed up for snow sports coaching.

Children

Where data on children is involved, all information is freely given to Snowbility by a parent or carer and is in relation to the company's main activity which is snow sports coaching for additional needs students.

Data breaches

The right procedures are in place to detect, report and investigate personal data breaches. All data is held on Snowbility's Zoho Creator system which is encrypted and backed by the Zoho Corporation.

Data Protection Office

Richard Fetherston, Managing Director of Snowbility, is the designated data protection officer.

International

Snowbility does not have any overseas data on its system related to students.

The Data Protection Act

The Data Protection Act controls how personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate
- Is kept for no longer than is necessary
- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the European Economic Area without adequate protection

Key policy related to additional needs

The welfare of children, young people and adults at risk is paramount and confidentiality must never prevent the sharing of information with appropriate and relevant persons or agencies, when not to do so may prevent appropriate safeguarding and place a child, young person and/or adult at risk, at risk of harm or abuse.

Data protection

All staff that work for Snowbility, whether at a centre or remotely, must:

- Keep all student information confidential and not disclose any data to other persons unless authorised to do so by Snowbility.
- Familiarise themselves with the provisions of the Data Protection Act 1998 and comply with its provisions.
- Familiarise themselves with Snowbility's Data Protection Policy No. ZA184282.
- Process personal data strictly in accordance with the Data Protection Act 1998, the Snowbility data protection policy and other policies and procedures issued by Snowbility.
- Comply with Snowbility's Code of Conduct policy

Snowbility views any breach of the Data Protection Act 1998, its Data Protection Policy and Code of Conduct Policy as gross misconduct, which may lead to summary dismissal under its disciplinary procedures.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

The Data Protection Act applies to all personal data held in filing systems, contact databases, emails, and portable media.

It includes any information that can be used to identify an individual such as photographs, contact names and addresses for employees, committee members, stakeholders, and others with whom we do business.

It also includes information processed on behalf of Snowbility by third parties.

Snowbility regards the lawful and correct treatment of personal information as essential to protect the interests of those whose personal data the company holds and to maintain confidence in its operations.

Accordingly, Snowbility will ensure that all personal information will be processed in accordance with the Data Protection Act 1998.

The Data Protection Principles

Snowbility will adhere to the eight principles of the Data Protection Act 1998 which require that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with data subjects' rights
- Secure
- Not transferred to countries outside the European Economic Area without adequate protection

Responsibilities

The Managing Director has overall responsibility for data protection within Snowbility. This authority is delegated to the Client Services Administrator who is responsible for day-to-day corporate compliance with the Data Protection Act and providing advice to staff.

Management of personal data

Personal data should only be collected where it is necessary for the work of Snowbility and should be kept to the minimum necessary for that task.

Staff must follow good practice for handling personal data as set out in the data protection Good Practice Guide:

- Snowbility will only use personal information where this is necessary to carry out its functions.
- Information solicited in response to website or other consultations will include an appropriate data protection statement at all gateways.
- Portable media that may contain personal data will be encrypted if held outside secure office premises based on a risk assessment.
- Sensitive, personal data will not be published on Snowbility's website apart from personal testimonials where the individual has provided explicit written consent.

Security of sensitive, personal data

Access to sensitive, personal data held in electronic form must be limited to a need to know basis and managed via appropriate permission's access on the Snowbility network.

Everyone managing and handling personal information is responsible for following good data protection practice in accordance with Snowbility's Data Protection Policy.

Any potential breach of security concerning loss, inappropriate disclosure or misuse of sensitive personal data such as through lost or stolen laptops must be reported to the Managing Director Snowbility.

Website

Snowbility will ensure that all relevant gateways soliciting information on the website have appropriate statements clearly explaining how personal data will be used by Snowbility.

Social media

Snowbility will ensure that all relevant information on social media have appropriate statements clearly explaining how personal data will be used by Snowbility.

Sharing personal data

Personal data may be shared with third parties where this is necessary for the performance of Snowbility's functions and in accordance with Snowbility's policy.

Disclosure of personal information under the Freedom of Information Act

In response to requests under the Freedom of Information Act ("the FOI"), Snowbilty may disclose staff personal data. In doing so, it will give due consideration to whether in all the circumstances the disclosure would be fair to the individual and balance its duty of care to staff in respect of protecting their personal information from unwarranted intrusion with its legal obligations to disclose information under FOI.

When handling FOI requests for personal information, there will be a presumption in favour of protecting personal privacy:

- No HR information will be disclosed except in response to an individual's access request.
- No personal email addresses, direct fax or DDIs will be disclosed.
- No names of staff will be disclosed except where they are in 'public facing roles'. Public facing roles are those where individuals deal directly with the public and where there is a legitimate expectation that their name should be known.
- Job titles of staff will generally be disclosed.
- Names only of Directors and Board members will be disclosed.
- No private addresses will be disclosed.

In applying this 'default' position, it is recognised that names and contact details of some staff are proactively placed in the public domain on the Snowbility website. Any such publicly available information will be disclosed.

Subject access requests

Any individual, including a member of staff, has a legal right of access to their personal data held by Snowbility under the Act. The Managing Director will be responsible for managing all individual's access requests by the public within statutory time frames including verification of the identity of the individual.

CONTRACTS

All contracts with third parties that involve the processing of personal data will include specific obligations to comply with the Data Protection Act 1998.

REVIEW

The Snowbility Data Protection Policy will be reviewed in February 2018.