General Data Protection Regulation (GDPR) Policy

Introduction

This General Data Protection Regulation (GDPR) Policy sets out OISE's commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

Policy Statement

OISE Ltd is committed fully to compliance with the requirements of the Data Protection Act 1998. The 1998 Act applies to all organisations that process data to their employees, as well as to others e.g. customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives rights to those whose data is being processed.

To this end, OISE Ltd endorses fully and adheres to the eight principles of data protection, as set out in the DPA.

1. Data must be processed fairly and lawfully.
2. Data must only be obtained for specified and lawful purposes.
3. Data must be adequate, relevant and not excessive.
4. Data must be accurate and up to date.
5. Data must not be kept for longer than necessary.
6. Data must be processed in accordance with the "data subject's" (the individual's) rights.
7. Data must be securely kept.
8. Data must not be transferred to any other country without adequate protection in place.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, OISE Ltd will:

- observe fully the conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the DPA (i.e., the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards.

Status of this Policy

The Policy does not form part of the formal contract of employment for staff but it is a condition of employment that staff will abide by the rules and policies made by OISE Ltd from time to time. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings. This Policy was approved on 17 October 2022. It will be reviewed no later than 17 October 2023

Designated Data Controllers

The Designated Data will deal with day-to-day matters. Any member of staff, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with Simon Pawley at simon.pawley@oise.com

Staff Responsibilities
All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date.
- informing your Line Manger, payroll/HR of any changes to information that they have provided, e.g., changes of address, either at the time of appointment or subsequently. The organisation cannot be held responsible for any errors unless the employee has informed it of such changes.

Data Security
All staff are responsible for ensuring that:

- any personal data that they hold is kept securely.
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Disaster Recovery

1. OISE Ltd backs up data every day and has multiple copies (at least one set for each day of the week and additional weekly ones in order to have at least a month's worth of data at any one time). Records of these are kept.
2. Backups are kept off site. Any kept on site are in special heat-proof safes: fire-proofing alone is inadequate.
3. Backups are verified regularly by the software and system supplier.
4. Master copies of software are stored off site or in a heat-proof safe.
5. Firewalls and virus checkers are kept up to date and running, and users are trained in virus avoidance and detection.
6. Computers are protected from physical harm, theft or damage, and from electrical surges using protective plugs.
7. OISE Ltd plans for how to deal with loss of electricity, external data links, server failure, and network problems. It uses paper forms where necessary for temporary record keeping.

Subject Consent
In many cases, the organisation can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the DPA (and to which special rules apply), express consent must be obtained.

Subject Access
An employee may request details of personal information which we hold about him or her under the DPA. A small fee may be payable and will be based on the administrative cost of providing the information. If an employee would like a copy of the information held on him or her, they should write to hr@oise.com. The requested information will normally be provided within one month.

If an employee believes that any information held on him or her is incorrect or incomplete, then they should write to or email as soon as possible, at the above address. The organisation will promptly correct any information found to be incorrect.

Conclusion

This policy sets out this OISE's commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

Signed: _____

Date: 17 October 2023 _____

Policy review date: 17 October 2024 _____