ICL Education Group GDPR Policy

BACKGROUND

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. Replacing the 1995 Data Protection Directive, this is the most significant update to international data protection law in two decades. Although the GDPR is a regulation in European Union (EU) law, businesses outside the EU must abide by its provisions if they wish to exchange data with EU entities. Because of the international nature of the ICL Education Group's business, it is important that ICL's own data protection conforms to the standards established by the GDPR.

The GDPR strengthens individuals' rights and brings corresponding new requirements on organisations to demonstrate data accountability, matched by new penalties for non-compliance. The GDPR provides additional limitations on the circumstances in which sensitive personal data may lawfully be processed, such as:

- in the area of public health (e.g., ensuring the safety of medicinal products),
- when data, deemed to be in the public interest, is considered for archiving for historical, scientific, research or statistical purposes

Sensitive personal data includes information about:

- racial or ethnic origins
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- personal sexual history and/or orientation

Under the 1995 Directive, personal data could only be transferred from an EU state to a non-EU state if the member state was satisfied with the adequacy of protection in respect of the particular transfer or set of transfers. Under the GDPR, however, the European Commission can certify adequacy of protection by a non-EU state on an ongoing basis.

STREAMLINING OF EU – NZ DATA TRANSFER

- The European Commission has recognised the adequacy of protection in New Zealand –one of only a small number of jurisdictions worldwide to achieve that
- New Zealand companies processing personally identifiable data concerning EU subjects must appoint a representative ("supervisory authority") in an EU member state to hear and investigate complaints about the handling of data.

GDPR

GDPR PRINCIPLES

The GDPR introduces six principles to replace those in the Data Protection Directive. These are that personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes deemed in the public interest, or for scientific, historical research or statistical purposes must not be incompatible with the initial purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, historical research or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

DATA SUBJECT RIGHTS

The GPDR provides a number of rights to data subjects. Each right is applicable in certain circumstances or conditions. Information about how these rights will be observed by the ICL Education Group is detailed below:

- **Right of access**: Individuals have a right to request a copy of any personal data that the ICL Education Group holds on them, and to request details regarding the use, retention and any relevant sharing of that data. This right of access is generally applicable, with exemptions only in specific, limited circumstances.
- **Right to rectification**: If personal data held by the ICL Education Group is inaccurate, out of date, or incomplete, individuals have the right to request the correction, update or completion of that data.

This right does not apply if the use or storage of the data is necessary for:

- compliance with a legal obligation, or for performance of a task carried out the in the public interest or in the exercise of official authority
- public health reasons
- for archiving in the public interest, scientific or historical research purposes or statistical purposes and erasure would seriously impair these objectives

- for the establishment, exercise or defence of legal claims exercising the right of freedom of expression and information

- **Right to erasure**: Individuals can request that personal data held by the ICL Education Group is erased or destroyed.

This right is applicable if:

- the data are no longer needed for the purposes for which they were collected
- consent was given to obtain the data and consent has been withdrawn
- the data subject objects to the processing and the ICL Education Group has no overriding legitimate grounds to keep the data
- the data has been unlawfully processed, e.g. the ICL Education Group cannot meet an appropriate processing condition for using/holding it
- the data must be erased to ensure compliance with a legal obligation.

- **Right to restriction**: Individuals can request that the use or storage of their data held by the ICL Education Group is restricted in a manner of the individuals' choosing.

This right is applicable if:

- the accuracy of personal data is contested by the data subject
- the use or storage of the data is unlawful and the data subject opposes erasure
- the ICL Education Group no longer needs the data but the individual needs the data for the establishment, exercise or defence of legal claims
- the individual has objected to the processing, and verification of the legitimate grounds of the ICL Education Group to override the objection is pending.

- **Right to data portability**: Individuals have the right to both receive their personal data in a structured, commonly used and machine-readable format and to transmit those data to another organisation.

- **Right to object:** Individuals have the right to object at any time to the use or storage by the ICL Education Group of their personal data.

This right is applicable if:

- the use or storage of the data is based on public interest tasks or legitimate interests
- the data are being used or stored for direct marketing purposes.

This right does not apply if the ICL Education Group has compelling legitimate grounds for the use or storage of the data which either override the interests, rights and freedoms of the individual, or are necessary for the establishment, exercise or defence of legal claims

- **Automated individual decision-making, including profiling**: Individuals have the right not to be subject to automated processing, including profiling.

This right is applicable if:

- the automated processing results in a decision with a legal or similarly significant effect on the individual

ASKING, RECORDING AND MANAGING CONSENT

Under the GDPR, a lawful basis needs to be identified and documented before data is processed. This is important as the lawful basis chosen will have a strong effect on an individual's rights e.g. where the ICL Education Group relies on consent to process data, an individual will have additional rights.

The rules around obtaining and evidencing such consent are stricter than previously. The checklist below will help ensure that the ICL Education Group gathers, records and manages consent in line with the new requirements under the GDPR.

It also provides a useful starting point for all ICL Education Group employees to update the way they process personal data.

Consent

- Check that consent is the most appropriate lawful basis for processing data.
- Make the request for consent prominent and separate it from our terms and conditions.
- Request people to positively opt in.
- Do not use pre-ticked boxes, or any other type of consent by default.
- Use clear, plain language that is easy to understand.
- Specify why we want the data and what we're going to do with it.
- Give granular options to consent to independent processing operations.
- Name our organisation and any third parties.
- Inform individuals about how they can withdraw their consent.
- Ensure that a person can refuse consent without detriment.
- Do not make consent a precondition of a service.
- If we offer online services directly to children, we should only seek consent to hold data about them if we have age-verification and parental-consent measures in place.

Recording consent

- Keep a record of when and how we obtained consent from every person.
- Keep a record of exactly what each person was informed about their data at the time.

Managing consent

- Regularly review consents to check that the relationship with the individual, the processing of their data and the purposes for which their data is held have not changed.
- Ensure that processes are in place to refresh consent at appropriate intervals, including for any required parental consents.
- Consider using privacy dashboards or other preference-management tools as a matter of good practice.
- Make it simple for individuals to withdraw consent at any time, and publicise how they can do so.

- Act on withdrawals of consent as soon as possible.
- Do not penalise individuals who wish to withdraw consent.

PERSONAL DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. If a personal data breach occurs, you must notify the national data protection authority for the relevant EU member state(s) within 72 hours "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

The notification needs to include:

- The nature of the breach
- Contact details for your data protection officer
- Likely consequences of the breach
- Mitigation measures put in place.

Any personal data breach or suspected personal data breach, or an accident or misuse involving personal data **must be immediately reported** to the ICL Education Group's Data Protection Officer at the address below:

Ewen Mackenzie-Bowie,
Chairman, ICL Education Group
ewen@icl.ac.nz
Tel +649 368 4343 | Fax +649 368 4949 | Mob +6421 780731
ICL Education Centre, 10-14 Lorne Street, Auckland CBD

If you are involved in or discover the breach, report it immediately to your Head of Service or Head of School Administration; they must then notify the Data Protection Officer and forward all relevant information related to the breach.

COST OF NON-COMPLIANCE

GDPR gives data protection authorities investigative and enforcement powers and the power to levy substantial fines (subject to jurisdictional limitations if you are wholly based in New Zealand).

Investigation power: An EU member state's data protection authority can order you to provide:

- any information and all personal data it requires for the performance of its tasks
- access to any premises in the EU where data processing equipment is situated.

Enforcement power: The EU member state's data protection authority can:

- issue warnings if your intended manner of processing is likely to infringe the GDPR
- issue reprimands, if your processing operations have infringed the GDPR
- order you to comply with the GDPR
- order that the flow of data to you from the EU be suspended
- impose a fine.

The fine is based on:

- the nature, gravity and duration of the infringement (e.g., number of affected people)
- whether the infringement was intentional or negligent
- whether you took steps to mitigate the damage
- whether you implemented technical and organizational measures to ensure compliance
- prior infringements
- the types of personal data involved
- the way the infringement became known.

Fines can be levied up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, or in the case of unlawful processing or infringement of the conditions for consent – up to €20 million or 4 % of annual turnover.