Definition of a Data Breach: Legally as per the EU's General Data Protection Regulations(GDPR), a data breach is defined as "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 (Article 4, Number 12)

Therefore, a data breach has occurred even if no harm is caused nor potentially caused and even if the data is not disclosed but rather destroyed, lost or changed.

Examples of personal data	**GDPR—private data** **(only those with a need to know in the performance of their jobs may have access)**	**NOT specifically GDPR but CAISL requires it to be kept confidential**
Contact Info (full name, address, personal email, telephone number, identified photograph)	YES	
Parental Custody	YES	
Health Information	YES	
Financial Data of any type, including salary/taxes/stipends (employee), billing/financial assistance/scholarships (parent)	YES	
Ed-Psych Testing	YES	
IEP/AP	YES	
An individual student's grades or any other reports (conduct, efforts, etc.)		YES
Collective Grades or other testing results for a group of students		This information will be shared BY THE DIVISION PRINCIPALS (or the teacher with DP approval) when the results are truly anonymized and statistically valid

Stage 1: **Data Breach suspected or notified by client or community member**
Responsibility: Every Individual
Time Frame: Immediate
When a staff member or member of the community believes that a breach as defined above may have occurred and/or is notified by any individual that a breach may have occurred, the person receiving the information will notify the IT Manager in person (or by telephone) and immediately send an email to privacy@caislisbon.org documenting the suspected breach with all available information.

The individual will NOT launch his/her own investigation.

Stage 2: **Evaluation of the suspected breach**
Responsibility: Information Technology Manager
Time Frame: As quickly as possible but no longer than 10 work days
The IT Manager will investigate to determine if a breach has occurred.

She is expected to consult with colleagues as required and colleagues are required to participate fully as needed in the investigation.

She is also expected to delegate the primary work of the investigation to an appropriate colleague should the suspected data breach not be IT-related. The person to whom the investigation is delegated will report all findings to the IT Manager and not take independent action outside of the investigation itself.

The investigation will include analysis of the harm which may have occurred or may occur in the future as a result of the breach, the possibility of ensuring that the breach is corrected and/or does not recur, and the intentionality of the breach.

If no data breach is determined to have occurred, the IT Manager will close the investigation, ensuring that the investigation is documented.

Stage 3: Correcting the Data Breach
Responsibility: IT Manager and Business Manager
Time Frame: Within 3 work days after the conclusion of the investigation
If Stage 2 determines that a data breach has occurred, the IT Manager and the Business Manager, in consultation with others as needed, will determine the next step.

The primary step in this case is always to correct the breach and regain data security as far as humanly and technologically possible. The IT Manager or Business Manager will ensure that those impacted or potentially impacted by the Breach and/or those who initially reported the Breach are informed of the results.

In most cases, where the breach (1) was contained, (2) no harm was done, and (3) there was no intentionality, no further action will be taken.

If any of the above three conditions were violated, the IT Manager and the Business Manager, in communication with the Director, will determine to whom the Breach needs to be reported which could include the Board of Trustees, the CNDP, and/or other agencies.