Data Breach Policy

DATA PROTECTION POLICY

MAY 2021

BRUCE COLLEGE
DATA BREACH POLICY

1 POLICY STATEMENT

Bruce College is committed to implementing a strong and effective Data Protection Policy and is fully aware of our obligations under the GDPR. The School recognises that data protection breaches can occur and this policy document clearly sets out our intent and reaction procedures for dealing with such incidents.

2 PURPOSE

The purpose of this policy is to provide the School's intent, objectives and procedures regarding data breaches involving the personal information that we hold for legitimate processing purposes. Technological and organisational measures have been put in place to ensure the security of all personal data that the School processes and all of our staff have been made aware of these processes and procedures. This policy sets out the procedures for the reporting, communicating and investigation of any such breaches and/or incidents.

3 SCOPE

This policy applies to all staff within the School and they have been made aware of their roles and responsibilities in terms of adherence to this policy and that not doing so may result in disciplinary action.

The General Data Protection Regulation's (GDPR) definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The School has a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the School.

3.1 OBJECTIVES

- To adhere to the GDPR and Irish Data Protection laws.
- To ensure that any data breaches are reported to the Supervisory Authority correct within the timeframes set out.
- To use breach investigations and logs to examine the reason why it/they occurred and to prevent any incidents occurring in the future.
- To protect the privacy of our staff and students.

- To ensure that the Supervisory Authority is notified of any data breach (*where applicable*) within the required timelines.

4 DATA BREACH PROCEDURES & GUIDELINES

In accordance with the School Data Protection Policy, there are measures in place to prevent data breaches occurring and for managing them in the rare event that they do occur.

4.1 BREACH MONITORING & REPORTING

The School has appointed a **[Data Protection Officer/Compliance Officer]** who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

4.2 BREACH INCIDENT PROCEDURES

4.2.1 IDENTIFICATION OF AN INCIDENT

As soon as a data breach has been identified, it is reported to the [**Data Protection Officer/Compliance Officer]** immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of the School. These procedures are for the protection of the School, its staff, students and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

4.2.2 BREACH RECORDING

The School utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder *(electronic or hard-copy)* and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the School Principal is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (*refer to section 6 of this policy*). The Supervisory Authority protocols are to be followed and their ***'Security Breach Notification Form'*** should be completed and submitted. In

addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

4.3 BREACH RISK ASSESSMENT

4.3.1 HUMAN ERROR

In all cases of a personal data breach, the School Principal will conduct an investigation into the causes of the said breach in order to ascertain the facts. That is to say, if the breach was caused by human or system error.

Accordingly, a review will be carried in and any gaps or lapses that have been identified or contributed to the error will be remedied to mitigate any recurrence. Such measures may include but are not limited to:

- Retraining of staff.
- Re-assessment of School procedures.
- Securing the office/building.
- Removal of security rights.
- The use of additional back-up measures to restore lost/stolen personal data.
- Changing of access rights, passwords codes etc.

4.3.2 ASSESSMENT OF RISK AND INVESTIGATION

The School Principal should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The investigator should look at: -

- The type and nature of personal data involved.
- The sensitivity of that personal data.
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident.

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

5 BREACH NOTIFICATIONS

The School recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the School's responsibilities and we have developed reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

5.1 SUPERVISORY AUTHORITY NOTIFICATION

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach **no later than 72 hours** after the School becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach.
- The categories and approximate number of data subjects affected.
- The categories and approximate number of personal data records concerned.
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information).*
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects).*

Breach incident procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

5.2 DATA SUBJECT NOTIFICATION

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach.
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information).*
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects).*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

6 RECORD KEEPING

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the School Principal and will be retained for a period of 6 years from the date of the incident.

7 RESPONSIBILITIES

The School will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The School Principal is responsible for regular review of the School's data protection policy and any follow-up requirements.