Checklist for Data Breach

Breach Notification Process Under GDPR

From 25th May 2018, the General Data Protection Regulation (GDPR) introduces a requirement for organisations, including schools, to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach. The supervisory authority is the Data Protection Commission in Ireland.

Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay.

To facilitate decision-making and determine whether or not your school needs to notify the relevant supervisory authority and affected individuals, you should have a high-quality risk management process and robust breach detection, investigation and reporting processes.

Prevention is better than Cure

Complying with the relevant reporting requirements following a data security breach is no substitute for the proper design of systems to secure personal data from accidental or deliberate disclosure.

Even with the best-designed systems, mistakes can happen!

As part of a data security policy, the school should anticipate what it would do if there were a data breach.

Some questions to consider:

•What would your school do if it had a data breach incident?

•Have you a policy in place that specifies what a data breach is? (It is not just lost USB keys/disks/laptops. It may include any loss of control over personal data entrusted to your school as an organisation, including inappropriate access to personal data on your systems or the sending of personal data to the wrong individuals).

•How would you know that your school had suffered a data breach? Does staff at all levels understand the implications of losing personal data?

•Has your school specified whom staff tell if they have lost control of personal data?

•Does your policy make clear who is responsible for dealing with an incident?

•Does your policy meet the requirements of the Data Protection Commissioner's approved Personal Data Security Breach Code of Practice? https://www.dataprotection.ie/docs/Data-Security-Breach-Code-of-Practice/y/1082.htm

A School's Self-Declared Risk Rating

In determining how serious you consider the breach to be for affected individuals, you should take into account the impact the breach could potentially have on individuals whose data has been exposed. In assessing this potential impact you should consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed. The levels of risk are further defined below:

- Low Risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
- Medium Risk: The breach may have an impact on individuals, but the impact is unlikely to be substantial
- High Risk: The breach may have a considerable impact on affected individuals
- Severe Risk: The breach may have a critical, extensive or dangerous impact on affected individuals.

Appendix One contains the Checklist

Appendix One: Data Breach Checklist for your school:

PREPARING FOR DATA PROTECTION BREACH	YES	NO	ADDITIONAL NOTES
We know how to recognise a personal data breach.			
We understand that a personal data breach is not only about loss or theft of personal data			
We have prepared a response plan for addressing any personal data breaches that occur.			
We have allocated responsibility for managing breaches to a dedicated person or team.			
Our staff knows how to escalate a security incident to the appropriate person or team in our school to determine whether a breach has occurred.			

RESPONDING TO A DATA BREACH	YES	NO	ADDITIONAL NOTES
We have in place a process to access the likely risk to individuals as a result of a breach.			
We know who is the relevant supervisory authority for our processing activities.			
We have a process to notify the Data Protection Commissioner's Office (DPCO) of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.			
We know what information we must give the DPCO about a breach.			
We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.			
We know we must inform affected individuals without undue delay.			
We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.			
We document all breaches, even if they don't all need to be reported.			

HOW TO REPORT A DATA BREACH	COMPLETED
All breach notification forms must be emailed to: breaches@dataprotection.ie	
All national breach notifications must be notified using the 'National Breach Notification Form'	
Contact the relevant supervisory authority of a breach within 72 hours of your organisation becoming aware of it.	
Directly contact individuals affected by a breach if it is likely to result in a high risk to their rights and freedoms. (Note: A 'high risk' means the threshold for notifying individuals is greater than notifying the relevant supervisory authority.)	
Complete a breach notification form using the 'National Breach Notification Form' Example of the information that will be required: • The categories and number of individuals affected by the breach • The categories and number of personal data records affected by the breach. • The name and contact details of the relevant person responsible for the school's data protection (Principal) or (Data Protection Officer in an ETB) or an additional contact where more information can be obtained. • A detailed description of the potential consequences of the data breach • A detailed description of what measures your school has taken or will take to address the data breach • A detailed description of the measures your school has taken or will take to mitigate any possible adverse effects to either itself or the individuals affected	
Breach notification emailed to: breaches@dataprotection.ie	

For further assistance:

Contact: …… Mobile…….. in our school

Contact: …… Mobile…….. in our school

For further information, visit:

https://www.dataprotection.ie/docs/GDPR-Overview/m/1718.htm