Data breach procedure

A data breach is any incident where a person's data is unlawfully lost, stolen, deleted, altered disclosed or otherwise processed in an unauthorised manner.

All data breaches must be recorded and certain breaches must be reported to the ICO (within 72 hours of the breach being discovered) and to the data subject (the person, or persons, whose data has been affected).

The severity of the breach, and the likely impact on the data subject, should be assessed in order to determine what action needs to be taken

If you experience a data breach, you must follow the steps outlined below;

- Contact the trust's DPO (Jason Smith) immediately on 01908 533 283, option 2, for advice
- Make a record of the breach on the breach record on your own school's GDPR compliance tracker (example form shown below)
- Do not disclose the details of the breach with any other parties until you have spoken to the DPO

Where a breach has occurred due to a gap in security, all possible steps must be taken to ensure that the gap is closed in order to prevent a reoccurrence of the breach.

Depending on the nature of the breach and the likely effect on the data subject, a decision will be made, in conjunction with the trusts data protection officer, as to whether the breach needs to be reported to the data subject or to the ICO.
There is a legal obligation to report breaches to the ICO within 72 hours of being discovered. It is critical, therefore, that all breaches are reported to the DPO as soon as they are discovered, so that this timeframe can be met.

For further advice, please contact dpo@iftl.co.uk

Inspiring Futures Through Learning

Ref	Details of Breach						Consequences of breach	Action taken			Entry made by & date
	Date of breach?	How many people affected?	Nature of breach?	Description of breach	How was breach discovered?	Description of data		Individuals informed?	Remedial action	ICO infomed	
Ex01 (Example Only)	*01/01/ 1970*	*50*	*Loss of data*	*Payroll data on USB stick left on train*	*Employee that lost USB stick reported the loss to office*	*Names, bank details, employee information*	*Identity theft, fraud, employee stress, reputational damage to organisation*	*Yes, by letter on 02/01/1970*	*Employees informed, payroll provider informed, employees advised to speak to banks re securing accounts, policy on memory sticks reviewed*	*Yes, on 02/01 by trust DPO*	*Jason Smith, 02/01/1970*