This policy lays out the responsibilities of individuals with respect to data management and protection as well as the procedures that are in place in the event of a data breach.

Winchmore Tutors is registered with the Information Commissioner's Office under registration number ZA09120.

Responsibilities

Information Users

It is the responsibility of all information users to report genuine, potential, suspected and threatened Data Protection Incidents and to assist with investigations as required, especially if urgent action is required to avoid additional damage.

Incident Management Staff

WT staff with specific responsibilities for receiving data breach and protection incident reports and for initiating investigations are:

- The Data Protection Officer
- The IT Manager

Data Protection Officer (DPO)

The DPO is solely responsible for deciding whether a report should be made to the Information Commissioners Office (ICO), whether other parties should be informed and for communication of the relevant information as required.

The DPO will maintain a record of all data incidents involving personal data irrespective of whether or not the incident is reported to the ICO as a data breach.

Breach Management

Data Protection Incidents must be reported immediately and notified by following the reporting guidance set out in this procedure:

- Incidents must be reported by sending an email to rdc@winchmoretutors.com
- The report should include full and accurate details of the incident including who is reporting it and what kind of data is involved.
- Once a data protection incident has been reported, an initial assessment will be made by the DPO to establish the veracity of the report and severity of the incident.

If the Data Protection Incident has any IT security elements – for example, a user account was compromised as part of a phishing campaign – the WT IT Manager must also be alerted.

Breach management has four critical elements:

- Containment and recovery – The goal is to limit any damage as far as possible
- Assess the ongoing risks – The assessment will help to guide decisions on which remedial actions have to be taken as well as who will have to be notified
- Notifying the appropriate people/organisations – This would only be done after an assessment has taken place and only by appointed staff
- Evaluation – Both of the incident at hand, the handling thereof, and whether mitigating steps can be taken to avoid a future occurrence of the same type of incident.

Activities and points for consideration by the responsible investigator when dealing with these four elements should be logged in an "Incident Checklist". An activity log be created to record the timeline of the incident management.

If a third-party organisation's data is affected, the department holding said data has to alert and consult the DPO and make sure that terms of use as part of the relevant contracts are adhered to.

Incident Review

The DPO will review incidents regularly, including whether the procedure was adhered to, to address possible reoccurrences of incidents and to address any new risks that were highlighted as part of the investigation.

The reviewing process will allow identifying necessary adjustments to the breach management procedure, to existing policies or the need for new policies.

Where deemed necessary, the DPO will make the required disclosure to the Information Commissioner's Office.

Data Classification

All reported incidents have to include the relevant data classifications so that the associated risks can be accurately assessed:

- **Public Data** – Information which is either intended for public use or which could be made public without any adverse impact on WT
- **Internal Data** – Information which is related to the day-to-day activities of WT. It is mainly intended for use by staff and students, although some data might be helpful to third parties working with WT
- **Confidential Data –** Information which is related to the more sensitive nature of procedures and processes of WT which represent the essential intellectual capital and knowledge. Access to this kind of information should only be granted to those people who need to know in order to fulfil the role within WT.
- **Highly Confidential Data or Personal Data –** Information that, would cause significant damage to WT's business activities or reputation, if it should be released. In the case of personal data would lead to a breach of the Data Protection Act 2018. Access to this kind of information should be highly restricted to staff which has the need and right to access and/or modify this specific set of data

Craig Varney : Winchmore Tutors - Director