Data Breach Policy

1. Introduction

This is the school's Data Breach policy which should be read alongside our Data Protection Policy.

To carry out the school's functions it is necessary to process personal data relating to our staff, pupils, parents, visitors and others.

Personal data is information relating to a living individual who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

The personal data the school processes includes special category data this is data which is of sensitive nature such as health information, racial or ethnic origin, biometric data and trade union membership.

2. What is a Personal Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

3. What responsibilities does the school have in relation to a personal data breach?

3.1 Notification to the ICO

The school is required by the UK GDPR to report certain types of personal data breach to the Information Commissioner's Office (ICO).

When a personal data breach has occurred, the school will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's **likely** that there will be a risk, then the school must notify the ICO, if it's unlikely then the school doesn't have to report it.

The school must report a notifiable breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

3.2 Communication with the affected individuals

The school is required by the UK GDPR to inform the affected individual(s) of certain types of personal data breach.

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, the UK GDPR requires the school to inform those concerned directly and without undue delay i.e. as soon as possible.

In addition to informing the individual about the nature of the personal data breach the school must provide them with information about:

- The name and contact details of our DPO for any queries.
- The likely consequences of the personal data breach.
- The measures taken/to be taken to address the breach including, where appropriate, measures to mitigate the possible adverse effects.

The school might not be required to notify the affected individual if certain exceptions apply.

3.3 Record keeping

The school will keep a record of any personal data breaches whether they are notifiable to the ICO or not, including the facts of the personal data breach, its effects and the remedial action taken.

4. School's processors

Some of the school's contractors e.g. our IT suppliers process personal data on behalf of the school. The UK GDPR requires suppliers who process data on our behalf to notify the school without undue delay after becoming aware of a personal data breach. Our processors are required by the terms and conditions of their contracts to assist the School with any personal data breaches.

5. The School's procedures

The school has a Cyber Response Plan in place for our staff which deals with:

- reporting data protection incidents

- investigating data protection incidents
- managing data protection incidents
- containing and/or recovering data
- assessing the risk
- notification to the ICO/individual
- recording data protection incidents and action taken

6. Training:

Our staff are provided with data protection training (which includes guidance on personal data breaches) and information on how to report a data protection incident and the school's policies and procedures relating to data protection and personal data breaches.

7. Contact:

Louise Rousell, the School's Data Protection Officer l.rousell@tavistock.hants.sch.uk, 01252 616778 can be contacted with any queries about this policy.