KING EDWARD VI
HIGH SCHOOL

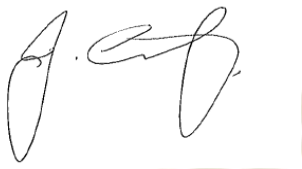
ADDRESS: Dryden Crescent, Stafford, ST17 9YJ
TEL: 01785 258546
WEB: www.kevi.org.uk
EMAIL: headteacher@kevi.org.uk
HEADTEACHER: Mr J Christey

KING EDWARD VI HIGH SCHOOL

INFORMATION AND SECURITY INCIDENT REPORTING POLICY

Encouraging and supporting all our learners to

"Be the best that they can be"



Head teacher

Mr J Christey

Governor

Mr C Soutar

Review Date **Every 3 years or as legislation changes**

Ofsted Good rating

Introduction

From May 2018 the UKs existing Data Protection Act will be replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of King Edward VI High School's preparation for this new legislation a new information policy has been developed.

This policy has been written to inform employees what to do if they discover an information security incident.

Queries about any aspect of King Edward VI High School's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer

Name:	Natalie Morrissey
Tel:	01785 278109
Email:	dpo@staffordshire.gov.uk

Scope

This policy applies to all King Edward VI High School's employees, any authorised agents working on behalf of the school, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including but not limited to

- Hard copy or documents printed or written on paper
- Information or data stored electronically including scanned images
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- Information stored on portable computing devices including mobile phones tablets cameras and laptops
- Speech, voice recordings and verbal communications including voicemail
- Published web content for example intranet and internet

- Photographs and other digital images

Article 33 of the GDPR requires data controllers to report breaches of personal data to the Information Commissioners Officer and sometimes the affected data subject(s) within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subjects(s).

Therefore, it is vital that King Edward VI High School has a robust system in place to manage, contain and report such incidents. The Information Security Management Policy details how the school will handle and manage information security incidents when they arise.

Notification and Containment

In order for the school to report serious incidents to the ICO within 72 hours it is vital that it has a robust system in place to manage, contain and report such incidents.

Immediate Actions (within 24 hours)

If an employee, Governor or contractor is made aware of an actual data breach or an information security event (a "near miss") they must report it to their line manager and the Data Manager within 24 hours. If the Data Manager is not at work at the time of the notification, then their out of office email will nominate another individual to start the investigation process.

If appropriate the officer who located the breach or their line manager will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information

Assigning Investigation (within 48 hours)

Once received the Data Manager will assess the data protection risks and assign a severity rating according to the identified risks and mitigations.

The severity ratings are

White	<u>Information Security Event</u> No breach has taken place but there is a failure of the implemented safeguards that could cause data breaches in the future
Green	<u>Minimal Impact</u> A data breach has occurred but has been contained within the Organisation (or trusted partner Organisation), the information is not considered to be particularly sensitive and no further action is deemed necessary
Amber	<u>Moderate Impact</u> Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the Information Commissioners Office
Red	<u>Serious Impact</u> A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial or physical damage) to individuals concerned. The breach warrants potential reporting to the Information Commission's Office and urgent remedial action. HR input may also be required

The Data Manager will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The Data Manager will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistant of the Internal Audit and Counter Fraud Teams.

Reporting to the ICO/Data Subjects (within 72 hours)

The SIRO in conjunction with the service manager, Data Manager, IAL and DPO will make a decision as to whether the incident needs to be reported to the ICO, and also whether any data subjects need to be informed. The Service Manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigation and Concluding Incidents

The Data Manager will ensure that all investigation have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the Council.

The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.