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

EXAMS GDPR POLICY

Encouraging and supporting all our learners to
"Be the best that they can be"

Headteacher

Mr J Christey

Charles Soutar

Governor

Mr C Soutar

Review Date **Annually or as legislation changes**

Key staff involved in the General Data Protection Regulation Policy

Role	Name
Head of Centre	Jason Christey
Exams Officer/Data Manager	Jacqueline Gray
Assistant Head with responsibility for Assessment	Emma Knights
Data Protection officer	Natalie Morrissey T: 01785 278109 E: dpo@staffordshire.gov.uk

Purpose of the Policy

This policy details how King Edward VI High School in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulation (GDPR).

Students are given the right to find out what information the centre holds about them, how this is protected, how this can be accessed and how data breaches are dealt with.

All exams office staff responsible for collecting and sharing candidates' data are required to follow strict rules called 'data protection principles' ensuring the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

To ensure that the centre meets the requirements of the DPA 2018 and GDPR, all candidates' exam information – even that which is not classified as personal or sensitive – is covered under this policy.

There is a requirement for the Exams Officer to hold exams-related information on candidates taking external examinations. For further details on the type of information held please refer to "*Section 6 – Candidate information, audit and protection measures*."

Candidates' exams-related data may be shared with the following organisations:

- Schools in the Stafford Sixth Form Partnership
- Awarding bodies
- Joint Council for Qualifications
- Department for Education; Local Authority; the Press (with the student's permission)

This data may be shared via one or more of the following methods:

- hard copy
- email
- secure extranet site(s) – eAQA; OCR Interchange; Pearson Edexcel Online;
- Management Information System (MIS) provided by Capita SIMS
- sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-a2c) to/from awarding body processing systems; etc.]

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post-results/certificate information.

Informing candidates of the information held

King Edward VI High School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via electronic communication and written communication
- given access to this policy via centre website and written request

Candidates are made aware of the above during their course of study leading to an externally accredited qualification.

At this point, the centre also brings to the attention of candidates the annually updated JCQ document Information for candidates – Privacy Notice which explains how the JCQ awarding bodies process their personal data in accordance with the DPA 2018 and GDPR.

Candidates eligible for access arrangements are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form (Personal data consent, Privacy Notice (AAO) and Data Protection confirmation) before access arrangements approval applications can be processed online.

Hardware and software

The table below confirms how IT hardware, software and access to online systems is protected in line with DPA & GDPR requirements.

Hardware	**Protection Measures**
Desktop computer Laptop Tablet	❖ Antivirus updated regularly ❖ Regular hardware checks / hardware access managed by security policy ❖ Externally managed Firewall (ISP) ❖ Internet access controlled internally via filter ❖ Access to applications managed by policy (i.e. word allowed / disallowed, spell check allowed / disallowed) ❖ Controlled assessments stored separately with separate user accounts

Software/Online system	**Protection Measures**
Active Directory (AD) Candidate information: Name	❖ protected / secure access to all servers ❖ rules for password setting ❖ SIMs administrator has to approve the creation of new user accounts and

Email address	determine access rights via user creation in SIMs
MIS – SIMs Candidate information: Everything	❖ protected usernames and passwords; ❖ rules for password setting ❖ centre administrator has to approve the creation of new user accounts and determine access rights
Go4Schools Candidate information: (Almost a replica of SIMs)	❖ protected usernames and passwords – as per AD ❖ rules for password setting – as per AD ❖ centre administrator has to approve the creation of new user accounts and determine access rights;
Awarding Bodies Candidate information	❖ protected usernames and passwords – as per awarding body ❖ Multi Factor Authentication for access to secure sites ❖ rules for password setting – as per Awarding body ❖ Exam Officer – responsible for sharing data as per awarding body

5. Dealing with data breaches

Although data is handled in line with DPA/GDPR regulations, a data breach may occur for any of the following reasons:

- loss or theft of data or equipment on which data is stored
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as a fire or flood
- hacking attack
- 'blagging' offences where information is obtained by deceiving the organisation who holds it

If a data protection breach is identified, the following steps will be taken:

Containment and recovery

The School Data Protection Officer will lead on investigating the breach.

Natalie Morrissey
T: 01785 278109
E: dpo@staffordshire.gov.uk

It will be established:

- who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This may include isolating or closing a compromised section of the network, finding a lost piece of equipment and/or changing the access codes
- whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back-up hardware to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts
- which authorities, if relevant, need to be informed

Assessment of ongoing risk

The following points will be considered in assessing the ongoing risk of the data breach:

- what type of data is involved?
- how sensitive is it?
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- regardless of what has happened to the data, what could the data tell a third party about the individual?
- how many individuals' personal data are affected by the breach?
- who are the individuals whose data has been breached?

- what harm can come to those individuals?
- are there wider consequences to consider such as a loss of public confidence in an important service we provide?

Notification of breach

Notification will take place to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

Evaluation and response

Once a data breach has been resolved, a full investigation of the incident will take place. This will include:

- reviewing what data is held and where and how it is stored
- identifying where risks and weak points in security measures lie (for example, use of portable storage devices or access to public networks)
- reviewing methods of data sharing and transmission
- increasing staff awareness of data security and filling gaps through training or tailored advice
- reviewing contingency plans

Candidate information, audit and protection measures

For the purposes of this policy, all candidates' exam-related information – even that not considered personal or sensitive under the DPA/GDPR – will be handled in line with DPA/GDPR guidelines.

An information audit is conducted annually.

The table below details the type of candidate exams-related information held, and how it is managed, stored and protected

Protection measures may include:

- password protected area on the centre's intranet
- secure drive accessible only to selected staff
- information held in secure area
- updates undertaken daily (this includes antivirus software, firewalls, internet browsers etc.)

Data retention periods

Details of retention periods, the actions taken at the end of the retention period and method of disposal are contained in the centre's Exams records management policy which is available/accessible from the school Exams Office.

A Records Management Retention Schedule is in use throughout the Admin team.

Access to information

Current and former candidates can request access to the information/data held on them by making a **subject access request** in writing with proof of I.D.to the school office. All requests will be dealt with within one month.

Third party access

Permission should be obtained before requesting personal information on another individual from a third-party organisation.

Candidates' personal data will not be shared with a third party unless already approved by parents in line with the whole school information policy

In the case of looked-after children or those in care, agreements may already be in place for information to be shared with the relevant authorities (for example, the Local Authority). The centre's Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

Sharing information with parents

The Centre will take into account any legislation and guidance regarding sharing information with parents (including non-resident parents), using guidance from the Department for Education (DfE) regarding parental responsibility and school reports on pupil performance:

- Understanding and dealing with issues relating to parental responsibility

  www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility/understanding-and-dealing-with-issues-relating-to-parental-responsibility

- School reports on pupil performance

  www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

Publishing exam results

When considering publishing exam results, the centre will make reference to the ICO (Information Commissioner's Office) Education and Families https://ico.org.uk/for-organisations/education/ information on *Publishing exam results*.