

**Kingswood House School**

General Data Protection Regulation policy (exams)

2018/19

This policy is annually reviewed to ensure compliance with current regulations

|  |  |
| --- | --- |
| Approved/reviewed by | |
| Katie Edwards | |
| Date of next review | September 2019 |

Key staff involved in the General Data Protection Regulation policy

|  |  |
| --- | --- |
| **Role** | **Name(s)** |
| Head of centre | **Mr Duncan Murphy** |
| Exams officer | **Mrs Katie Edwards** |
| Exams officer line manager (SLT) | **Mrs Sally Witts** |
| Privacy and Compliance Officer | **Mrs Katie Edwards** |
| IT manager | **Mrs Pippa Webb** |

Purpose of the policy

This policy details how Kingswood House 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.

Section 1 – Exams-related information

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 5 – Candidate information, audit and protection measures*.

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

* Awarding bodies
* Joint Council for Qualifications
* Department for Education or Local Authority

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

* hard copy
* email
* secure extranet sites – e.g. eAQA, OCR Interchange and Pearson Edexcel Online etc.
* the Schools Management Information System (MIS) provided by Double First (engage) 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.

Section 2 – Informing candidates of the information held

Kingswood House School ensures that candidates are fully aware of the information and data held.

All candidates are:

* informed via electronic communication and exams booklets.
* given access to this policy via the schools website

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.

Section 3 – 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 | Date of purchase and protection measures | Warranty expiry |
| Exams Officer & Senco both have a Laptop | Exams Officer laptop - Date of Purchase: September 2018.  Senco laptop – Date of Purchase September 2017 but completely wiped and rebuilt for reissue September 2018.  Both have up to date antivirus (Sophos) and firewall protection. | N/A |
| USB Sticks | Only used for exams laptop users. Candidate and Invigilator/Exams Officer stay with USB stick at all times until wiped. Wiped after use and checked before use by Exams Officer. Only used for GCSE’s and lock away in Secure Room. | N/A |

|  |  |
| --- | --- |
| Software/online system | Protection measure(s) |
| School network secure drive. | Restricted access to Exams Officer drive and Senco’s drive. Password protected with a mix of upper/lower case letters and numbers. Regular checks to Firewall and Antivirus software by IT department. |
| Awarding body secure extranet site(s) | Protected with usernames and passwords that are a mix of upper/lower cases letters and numbers. Exams Officer to approve the creation of new user accounts and determine access rights. Regular checks to Firewall and Antivirus software by IT department. |

Section 4 – 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:

1. **Containment and recovery**

Sally Witts, Bursar and Katie Edwards, Privacy and Compliance Officer will lead on investigating the breach.

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

1. **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?

1. **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.

1. **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

Section 5 – 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 every [XX] months (this may include updating antivirus software, firewalls, internet browsers etc.)

Section 6 – Data retention periods

Details of retention periods, the actions taken at the end of the retention period and method of disposal are contained in Kingswood House Exams archiving policy, which is accessible from the Schools Website or via the Exams Officer.

Section 7 – Access to information

Current and former candidates can request access to the information/data held on them by making a **subject access request** to Privacy and Compliance Officer in writing/email and ID will need to be confirmed if a former candidate is unknown to current staff. All requests will be dealt with within 40 calendar days.

**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 a request is accompanied with permission from the candidate and appropriate evidence (where relevant), to verify the ID of both parties, provided.

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 School’s Bursar will confirm the status of these agreements and approve/reject any requests.

**Sharing information with parents**

|  |
| --- |
| Kingswood House School would require parents to meet the above ‘Third party access’ requirements before we will be able to share exam results for their child.  Kingswood House School will take into account any other legislation and guidance regarding sharing information with parents (including non-resident parents), as example 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](https://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](http://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. |