AYLESBURY GRAMMAR SCHOOL

SCHOLA AILESBURIA

Founded in 1598

DATA PROTECTION EXAMINATIONS POLICY

This version was approved by the governing body July 2018
The next update will be due by July 2021

Signed:______________________________
J Collins - Chairman of Governors

1. Purpose of the policy

1.1 This policy details how Aylesbury Grammar School (the "centre"), in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act (DPA) and General Data Protection Regulation (GDPR).

1.2 This policy should be read in conjunction with the school's main Data Protection Policy

1.3 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.

1.4 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

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

2. Exams-related information

2.1 There is a requirement for the exams office 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)*.

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

- Awarding bodies
- Joint Council for Qualifications
- any other organisations as relevant to the centre e.g. Department for Education; Local Authority

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

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

2.4 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.

3. Informing candidates of the information held

3.1 Aylesbury Grammar School ensures that candidates are fully aware of the information and data held.

3.2 All candidates are:

- informed via suitable communication methods
- given access to this policy via centre website

3.3 Candidates are made aware of the above at the start of their course of study leading to external examinations.

4. Data security and storage of records

4.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

4.2 In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT Acceptable Use Policy)

4.3 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

5. Dealing with data breaches

5.1 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

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

Containment and recovery

5.3 The school’s Data Protection Officer (DPO) will lead on investigating the breach.

5.4 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

5.5 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

5.6 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

5.7 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

6. Candidate information, audit and protection measures

6.1 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.

6.2 An information audit is conducted regularly by the DPO.

6.3 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 as soon as possible from their release (this may include updating antivirus software, firewalls, internet browsers etc.)

7. Data retention periods

7.1 Details of retention periods, the actions taken at the end of the retention period and method of disposal are contained in the centre’s main Data Protection Policy which is available/accessible from the school’s website.

8. Access to information

8.1 Current and former candidates can request access to the information/data held on them by making a **subject access request** to the school’s Data Protection Officer in writing, email or Fax and ID may be required if a former candidate is unknown to current staff. All requests will normally be dealt with within 1 month – the school’s Data Protection Policy gives more details to the process..

Third party access

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

8.3 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.

8.4 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.