eat.uk.com

@EthosAcadTrust

Company Registration Number: 10745840 (England and Wales)

Ethos Academy Trust

Data Protection (Exams)

2023 - 2024

ETHOS COLLEGE

Nurturing inclusive learning communities

ETHOS ACADEMY TRUST

1	**Summary**	This policy details how Ethos College, 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).				
2	**Responsible person**	Head of Centre				
3	**Accountable ELT member**	Rebecca Smith				
4	**Applies to**	Ethos College				
5	**Trustees and/or individuals who have overseen development of this policy**	N/A				
6	**Headteachers/Service Heads who were consulted and have given approval (if applicable)**	Rebecca Smith				
8	**Ratifying committee(s) and date of final approval**	Head Teacher				
9	**Version Number**	1.3				
10	**Available on**	**Every**	**Y/N**	**Trust Website** **Academy Website** **Staff Portal**	**Y/N** **Y/N** **Y/N**	
11	**Related documents (if applicable)**					
12	**Disseminated to**	Entire College				
13	**Date of implementation (when shared)**					
14	**Date of next formal review**	November 2024				
15	**Consulted with Recognised Trade Unions**	N/A				

Date	Version	Action	Summary of changes
19/09/23	1.3	No Changes	

Contents

Section	Description	Page
1.	Purpose of the policy	3
2.	Exams related Information	3
3.	Informing candidates of the Information held	4
4.	Hardware and software	4
5.	Dealing with data breaches 5.1 Containment and recovery 5.2 Assessment of ongoing risk 5.3 Notification of breach 5.4 Evaluation of response	4 - 5
6.	Candidate Information, audit and protection measures	5
7.	Data retention periods	6
8.	Access to Information 8.1 Requesting exam Information 8.2 Responding to requests 8.3 Third party access 8.4 Sharing Information with parents/carers/guardians	6

1. Purpose of the policy

This policy details how Ethos College, 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).

> At the date of reviewing these regulations, although the UK has left the European Union the General Data Protection Regulation still has a direct effect within the UK (JCQ's General Regulations for Approved Centres (GR, section 6.1) **Personal data**)

Candidates 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.

2. Exams-related information

There is a requirement for the exams officer to hold exams-related information on candidates taking external examinations.
Candidates' exams-related data may be shared with the following organisations. Please note that this list is not exhaustive:

- Awarding bodies
- Joint Council for Qualifications
- Department for Education
- Local Authority
- The school at which a candidate is dual registered (where applicable)
- The Virtual School responsible for any pupil in care (where applicable)
- Sixth Form / further education colleges / apprenticeship providers (only when we are required to verify results)

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

- hard copy
- email
- secure extranet site(s) – e.g. e-AQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; NCFE Portal; ASDAN

- a Management Information System (MIS) provided by Schoolpod sending/ receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-a2c) to/from awarding body processing systems; etc.
- telephone – always by ringing back to verify identity

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

Please refer to the Ethos Academy Trust Data Protection Policy / GDPR Policy for more information.
Candidates are provided with a copy of 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. This is an appendix to the Candidate Exams Handbook, which is issued to candidates before they sit any exams. It is also published on the Ethos College website: (https://www.ethoscollege.uk.com/parents-pupils/exams/)
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.

4. Hardware and software

Please refer to the Ethos Academy Trust Data Protection Policy / GDPR Policy for more information.
Hardware and software requirements are covered by the GDPR Data Audit.

5. Dealing with data breaches

Please refer to the Ethos Academy Trust Data Protection Policy / GDPR Policy for more information.
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:

5.1 Containment and recovery

The Data Protection 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

5.2 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?

5.3 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.

5.4 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

6. 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.

All candidate information is stored securely in lockable cabinets, on the secure server or an encrypted memory stick. The building is secure and alarmed, the office and the cabinets within it are locked, and the exams safe is locked within a locked room (to comply with exam regulations).

Digital impact assessments will be conducted as required.

Data 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 automatically (this may include updating antivirus software, firewalls, internet browsers etc.)

7. 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 Archiving Policy, which is available from the Exams Officer.

8. Access to information

Please refer to the Ethos Academy Trust Data Protection Policy / GDPR Policy for more information.
The GDPR gives individuals the right to see information held about them. This means individuals can request information about them and their exam results, including:

- their mark
- comments written by the examiner
- minutes of any examination appeals panels

This does not however give individuals the right to copies of their answers to exam questions. For further information please see: https://ico.org.uk/your-data-matters/schools/exam-results/

8.1 Requesting exam information

Requests for exam information can be made to the Head of Centre in writing. If a former candidate is unknown to centre staff the candidate will be asked to present current photographic ID.

A decision will be made by head of centre as to whether the student is mature enough to understand the request they are making, with requests considered on a case by case basis. The Head of Centre will discuss the request with the Data Protection Officer.

8.2 Responding to requests

If a request is made for exam information before results have been announced, a request will be responded to:

- within five months of the date of the request, or
- within 40 days from when the results are published (whichever is earlier).

If a request is made once exam results have been published, the individual will receive a response within one month of their request.

8.3 Third party access

Permission will 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, is provided].

In the case of Children Looked After or those in care, agreements are already in place for information to be shared with the Local Authority).

8.4 Sharing information with parents/carers/guardians

The centre will take into account any other legislation and guidance regarding sharing information with parents/carers/guardians (including non-resident parents), for example guidance from the Department for Education (DfE) regarding parental responsibility and school reports on pupil performance.