# GENERAL DATA PROTECTION REGULATION POLICY (EXAMS)

| | |
|---|---|
| Updated | April 2018 |
| Approved by Principal | Yes |
| Review Date | April 2019 |
| Key Staff | Vice Principal, Curriculum, Attendance & Exams Manager, Exams Officer |
| Lead Staff for Review | Vice Principal |

# Table of Contents

## Key staff involved in the General Data Protection Regulation policy

| Role | Name(s) |
|---|---|
| Head of centre | Craig Wilson |
| Exams officer | Jasmine Robinson |
| Exams officer line manager (Senior Leader) | Dominic Tomalin<br>Carly Robinson |
| Data Protection Officer | Lisa Tyler |
| IT manager | Aaron Endersbe |
| Data manager | Valentina Calvi |

## Purpose of the policy

This policy details how CATS Cambridge (as part of Cambridge Education Group ("CEG")), in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 1998 until 24th May 2018 and the GDPR thereafter.

Students are given the right to find out what information (including personal data as defined in the GDPR)[1] 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 (including personal data) are required to follow strict rules called 'data protection principles' ensuring the information is:

- processed fairly, lawfully and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and not excessive in relation to the purposes for which it is processed
- accurate and where necessary kept up to date
- kept (in a format which identifies candidates) for no longer than is absolutely necessary
- kept safe and secure, including protecting against unauthorised or unlawful processing and against accidental loss, destruction or damage

In addition, a candidate's personal data will not be transferred outside the European Economic Area without adequate protection being put in place.

[1] any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 (1) GDPR)

To ensure that the centre meets the requirements of the GDPR, all candidates' exam information, even that which is not classified as personal or special category[2], is covered under this policy.

## Section 1 – Exams-related information

There is a requirement for the Exams Office(r) 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 external bodies.

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- Centre for Evaluation & Monitoring (CEM), Independent Schools Council (ISC), Independent Schools Inspectorate (ISI), British Council, Cambridge English Language Assessment, Department for Education, universities

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; CIE Direct.
- Management Information System (MIS) provided by Capita Unit-e, 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

CATS Cambridge ensures that candidates are fully aware of the information and personal data held by the centre.

All candidates are:

- informed via information pack given once entries made
- given access to this policy via written request

Candidates are made aware of the above once they have been entered for external examinations.

## Section 3 – Hardware and software

[2] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9(1) GDPR).

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

| Hardware | Protection measures | Warranty expiry |
|---|---|---|
| PC – Dell | Encrypted disks; administrator access restricted to IT Staff; PC protected by real time Sophos antivirus; monthly security updates automatically deployed via MDT; users access profiles created for role specific requirements; user password policy rigorously enforced.<br><br>Data transfer via Internal/External networks pass through successive levels of filtering and content/email checking to block Malware/Suspicious attachments and files | N/A<br><br>Majority of equipment is out of warranty – security and protection is carried out by system/security/process not warranty which is for repair |
| Laptop – Dell | As above | N/A |
| Laptop – Microsoft | As above | N/A |
| Server Systems – Dell | Systems host key business software applications that support the academic operation.<br><br>These servers are hosted in secure, dedicated Datacentres located in two principle CEG sites.<br><br>These systems have restricted administrator access, full back-up regime, and user access to data is controlled by full AD authentication. Full event logging is in place.<br><br>External access to networks and by detault all IT equipment is protected by a combination of layers of security.<br><br>Every network perimeter point has a firewall (eithera Cisco and Fortinet). All Ciscos conduct URL filtering using Cisco Firepower, Fortigate utilise | Full support and maintenance agreement for all critical business systems |

| | | |
|---|---|---|
| | Fortigard for content restriction and alerting.<br><br>Data centres run a sourcefire module between the LAN and DC network.<br><br>Egress filtering is all done via the Firepower rating system, destinations limited via DNS entries being locked down and restricting access. All secure configs are backed up using Solarwinds network config manager, and config backups compared against daily backups to highlight and alert against changes.<br><br>Live changes are captured in Solarwinds and alerting set up. SSH and HTTPS secure authentication,and running SNMP V3, access to management infrastructure is via its own locked down subnet with limited user access.<br><br>Admin interfaces are accessible via the internet ,and limited to specfic external IPs. | |
| User system security | Regularly reviewed and monitored.<br><br>Inactive or no longer required accounts are diasabled and held in a graveyard account. Archive and deletion is depending on users role and need for making data available for ex- students.<br><br>Passwords are valid for 90 days then are complusory changed, they must be a minimum of 12 mixed characters and cannot re-use the 5 previously used password. | |
| Data Transfer – WIFI | All systems transferring data via corporate WIFI are encrypted to | |

| | | |
|---|---|---|
| | WPA2 Enterprise level. Guest WIFI access is via a PSK key | |

| **Software/online system** | **Protection measure(s)** |
|---|---|
| [Insert details of any software or system used where candidate information is stored] | [Insert the measures in place to protect the information from unauthorised/unlawful access (liaise with the IT/Data manager to determine these)] |
| [Insert each as a new row in the table. Examples might include: MIS; Intranet; Internet browser(s); Awarding body secure extranet site(s); A2C; etc.] | [Example measures might include: protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers); rules for regularity of password changing; centre administrator has to approve the creation of new user accounts and determine access rights; regular checks to Firewall/Antivirus software; etc.] |
| Capita UNIT-e MIS | We are aware of what data we store, and the level of sensitivity. All databases are reliant on network security and perimeter control. Access controls are in place and monitoring of the server event logs.<br><br>Administrator accounts regularly reviewed and monitored. Restricted access to admin level privileges. Access requests go through an approval process. Local admin rights restricted to reduce client's ability to run executables.<br><br>Inactive or no longer required user accounts are disabled and held in a graveyard account. Archive and deletion is depending on user's role and need for making data available for ex-students.<br><br>Applications are monitored and logged using Solarwinds. Live changes are captured in Solarwinds.<br><br>Anti-malware detection and eradication using Sophos AV which is installed on all Client machines.<br><br>All server systems are patched in monthly maintenance windows to ensure that all appropriate system updates and security patches are applied.<br><br>Every perimeter has a firewall and URL filtering. |

| | |
|---|---|
| | Configs are backed up using Solarwinds network config manager, and config backups compared against daily backups to highlight and alert against changes.<br><br>Admin interfaces are accessible via the internet and limited to specific external IPs.<br><br>We engage an external security firm to conduct penetration testing on CEG systems and conduct regular internal testing using proprietary tools. |
| CEG Shackleton Staff Portal | As Above.<br><br>Access control via AD authentication<br><br>Password Policy in place - Passwords are valid for 90 days then are compulsorily changed, they must be a minimum of 12 mixed characters and cannot re-use the 5 previously used passwords. |
| CEG Ernest Student Portal | As Above. |
| Internet browser(s) | Currently we do not operate restrictions to a single browser due to limitations within 3rd Party applications targeting specific browsers.<br><br>Browsers used within CEG are Chrome, Firefox, Safari and IE. Automatic updates are applied and certain administrative functions are locked down.<br><br>URL Filtering is employed across CEG to restrict content access.<br><br>Firewalls restrict access to the ports made available. Hosts are locked down, and networks are segmented. |
| Awarding body secure extranet site(s); A2C, eAQA; OCR Interchange; Pearson Edexcel Online; CIE Direct | |

## Section 4 – Dealing with personal data breaches

Although personal data is handled in line with the GDPR, sometimes a personal data breach may still occur for any of the following reasons:

- loss or theft of data or equipment on which personal 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 personal data is obtained by deceiving the organisation who holds it

If a personal data breach is identified, the centre must immediately notify CEG's Data Protection Officer ("DPO"). The DPO will take the lead with the following steps:

**1. Assessment of whether a personal data breach needs to be notified**

The DPO will assess whether the personal data breach needs to be notified to the Information Commissioner's Office (ICO) and to individual candidates.

In both cases, the DPO will make a recommendation to the CEG executive team regarding notification in line with the GDPR and official guidance on personal data breach notification. The executive team will decide whether to notify and their decision will be final. Both the DPO's recommendation and the CEG executive team's decision will be recorded as part of CEG's accountability obligations under the GDPR.

**2. Containment and recovery**

It will be established:

- who needs to be made aware of the breach internally 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 personal data or ensuring that staff recognise when someone tries to use stolen data to access accounts

**3. Assessment of ongoing risk**

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

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

- who are the individuals whose personal 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 the centre provides?

**4. Evaluation and response**

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

- reviewing what personal 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 sharing of personal data and transmission
- increasing staff awareness of security when handling personal data and filling gaps through training or tailored advice
- reviewing contingency plans
- documenting the facts relating to the personal data breach, its effects and remedial action taken to ensure CEG's compliance with the accountability requirements of the GDPR.

## 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 special category under the GDPR – will be handled in line with 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 include:

- secure drive accessible only to selected staff
- secure destruction of data once deadline for retention has passed
- Password policies
- Anti-malware software

## 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 the centre's Exams archiving policy which is accessible via the Exams Policy on Shackleton or by requesting a copy from the Exams Officer.

## Section 7 – Access to information

Current and former candidates can request access to the personal data held on them by making a **subject access request** to the Data Protection Officer in writing/email. The email address from which the request comes from will be cross-checked against the student record on Shackleton. If the email address does not appear on the student record, then the candidate will need to confirm their identity by scanning and emailing a colour copy of their passport and a recent utility bill. Requests will be dealt with within 1 month.

**Third party access**

Permission should be obtained before requesting personal data 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. Permission must be provided in the form of an email from a verified email address on the student's record.

In the case of looked-after children or those in care, agreements may already be in place for personal data 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.

## Section 8 – Table recording candidate exams-related information held

For details of how to request access to information held, refer to section 7 of this policy (**Access to information**)

For further details of how long information is held, refer to section 6 of this policy (**Data retention periods**)

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| Access arrangements information | Information collected by ALS coordinator to process access arrangements | Candidate name<br>Candidate DOB<br>Gender<br>Data protection notice (candidate signature)<br>Diagnostic testing outcome(s)<br>Specialist report(s) (may also include candidate address)<br>Evidence of normal way of working | Access arrangements online<br>Shackleton<br>Lockable metal filing cabinet<br>R:Drive ALS folder | Secure user name and password<br>In secure area solely assigned to members of staff<br>Only accessible to Exams staff<br>Only accessible to Exams staff | Retained as long as pupil records are as defined in the CEG Retention Policy |
| Attendance registers copies | Registers record attendance at each written exam, are kept with seating plan and exam room incident log | Candidate name<br>Candidate number<br>Presence at exam | Lockable filing cabinet | Only accessible by EO staff | To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| | | | | | for the relevant exams series. |
| Candidates' work | Controlled assessments, coursework and non-examination assessments | Candidate name<br>Candidate number<br>Candidate marks and grades | Secure storage | Only accessible by EO staff | Retained until the post-results period has been completed for that exam series |
| Certificates | Record of achievement | Candidate name<br>Candidate number<br>UCI number<br>Candidate ODB<br>Candidate marks and grades | Lockable filing cabinet | Only accessible by EO staff | Retained securely for a minimum of 12 months from date of issue. |
| Certificate destruction information | A record of unclaimed certificates that have been destroyed. | Candidate name<br>Candidate number<br>UCI number<br>Candidate ODB<br>Candidate marks and grades | In Examinations R:Drive > Archive | Only accessible by EO staff | To be retained for 4 years from the date of certificate destruction. |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| Certificate issue information | A record of certificates that have been issued to candidates. | Candidate name<br>Candidate number<br>Candidate qualifications | Certificate collection file. Copies of post receipts or students sign-out in person, scanned and saved in file. | Only accessible by EO staff | Indefinite |
| Entry information | A record of which qualifications candidates have been entered for. | Candidate name, number, CEG number, preferred name, personal tutor, programme of study, qualification information | In Examinations R:Drive > Entries folder in each academic year | Only accessible by EO staff and emailed to Head of Centre and VP | Retained until the post-results period has been completed for that exam series |
| Exam room incident logs | Logs detailing the chronological activity happening in exam rooms from start to finish | Candidate name<br>Candidate number<br>Candidate toilet breaks | With the corresponding attendance register and seating plan in lockable filing cabinet | Only accessible by EO staff | To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series. |
| Overnight supervision information | Copy of JCQ form Timetable variation and | Candidate name | In Exams R:Drive | Only accessible by EO staff | To be retained indefinitely for |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| | confidentiality declaration for overnight supervision for any candidate eligible for these arrangements. | Candidate number<br>Candidate address | | | JCQ inspection purposes. |
| Post-results services: confirmation of candidate consent information | Hard copy or email record of candidate consent for an EAR or ATS request to be submitted to an awarding body | Candidate name<br>Candidate number<br>Candidate results information | Post-results services file for relevant academic year | Only accessible by EO staff. Only shared with HOD and VP/Head of Centre. | EAR consent to be retained for at least six months following the outcome of the enquiry or any subsequent appeal.<br>ATS consent to be retained for at least six months from the date consent given. |
| Post-results services: requests/outcome information | Any hard or digital copies of information relating to a post-results service request (EARs, appeals, ATS) submitted to an | Candidate name<br>Candidate number<br>Candidate results information | Post-results services file for relevant academic year | Only accessible by EO staff. Only shared with HOD and VP/Head of Centre. | Retained for at least six months following the outcome of the enquiry or any |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| | awarding body for a candidate and outcome information from the awarding body. | | | | subsequent appeal. |
| Post-results services: scripts provided by ATS service | Copy, digital or original exam scripts returned to the centre by the awarding body. | Candidate name<br>Candidate number<br>Candidate results information | Where scripts are retained by the centre, they are securely stored (including any electronic versions) and not edited in any way or disposed of until after the awarding body deadline. | Only accessible by EO staff. | n/a returned to the requester after the post-results period is complete |
| Post-results services: tracking logs | A log tracking to resolution all post-results service requests submitted to awarding bodies. | Candidate name<br>Candidate number<br>Candidate results information | Post-results services file for relevant academic year | Only accessible by EO staff. | Retained for at least six months following the outcome of the enquiry or any subsequent appeal. |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| | | | | | |
| Private candidate information | Any hard or digital copy information relating to private candidates' entries. | Candidate name, address, candidate number, email, phone number, date of birth and gender | In Exams R:Drive > Entries | Only accessible by EO staff. | To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series. |
| Resolving clashes information | Any information relating to the resolution of a candidate's clash of exam papers or a timetable variation. | Candidate name, candidate number | In Exams R:Drive > Entries | Only accessible by EO staff. | To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series. |
| Results information | Broadsheets of results summarising candidate | Candidate name, candidate number, DOB, gender, result information | In Exams R:Drive > Results for the | Only accessible by EO staff. | Records for current year plus previous 6 years |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| | final grades by subject by exam series. | | relevant academic year | | to be retained as a minimum. |
| Seating plans | Plans showing the seating arrangements of all candidates for every exam taken. | Candidate name<br>Candidate number<br>Candidate toilet breaks | With the corresponding attendance register and incident log in lockable filing cabinet | Only accessible by EO staff | To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series. |
| Special consideration information | Any hard or digital copies of information relating to a special consideration request and supporting evidence submitted to an awarding body for a candidate. | Candidate name<br>Candidate number<br>Candidate date of birth<br>Candidate medical information | Lockable filing cabinet | Only accessible by EO staff | To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series. |
| Suspected malpractice reports/outcomes | Any hard or digital copies of information relating to a suspected malpractice investigation/report | Candidate name<br>Candidate number | On Exams R:Drive, filed by Academic Year > Malpractice | Only accessible by EO staff, VP | To be kept until the deadline for EARs and the resolution of any |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| | submitted to an awarding body and outcome information from the awarding body. | | | and Head of Centre | outstanding enquiries/appeals for the relevant exams series. |
| Transfer of credit information | Any hard or digital copies of information relating to a GCE AS transfer of credit arrangement (for a legacy unitised GCE AS specification) application submitted to an awarding body for a candidate. | Candidate name<br>Candidate number<br>Candidate UCI | In Exams R:Drive > Transfer of credit | Only accessible by EO staff, VP and Head of Centre | To be retained until the issue of the GCE A level result for the candidate. |
| Transferred candidate information | Any hard or digital copies of information relating to an application for a transferred candidate arrangement submitted to an awarding body for a candidate. | Candidate name<br>Candidate number<br>Candidate UCI | In Exams R:Drive > Transfer of credit | Only accessible by EO staff, VP and Head of Centre | To be retained until the transfer arrangements are confirmed by the awarding body. |

| Information type | Information description (where required) | What personal/ special category data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|---|
| Very late arrival reports/outcomes | Any hard or digital copies of information relating to a very late arrival report submitted to an awarding body for a candidate and outcome information from the awarding body. | Candidate name<br>Candidate number | In Exams R:Drive > Academic Year > Very late arrivals | Only accessible by EO staff, VP and Head of Centre | To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series. |