Policy Document

# General Data Protection Regulation (GDPR) policy and process

# Table of Contents


Introduction ..... 3
Scope ..... 3
Aim ..... 3
Data Protection Act ..... 4
AQ staff responsibilities ..... 4
Your rights ..... 5
Definition of data breach ..... 5
Cyber security ..... 6
Artificial intelligence ..... 7
Assessment related data activity ..... 7
Recording of assessment ..... 7
Learner identification ..... 7
Learner consent ..... 8
GDPR Data Controllers and Data Processors ..... 8
Data Classification ..... 8
Data Security Breach Reporting ..... 9
External identification ..... 9
Internal identification ..... 9
Data Breach Management Plan ..... 9
References ..... 10
Policy updating and reviewing ..... 10
Policy version and owner ..... 10
Appendix A: Data Breach Management Plan ..... 11
Appendix B: Data Breach Incident Report Form ..... 13
Appendix C: Evaluation of Incident Severity and Checklist ..... 14
Appendix D: Example Format of Timeline of Breach ..... 15

## Introduction

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation and sharing of data and information grows, there are infinitely more ways by which data can be breached. Aspire Qualifications (AQ) is duty bound to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

## Scope

This policy applies to all AQ information, regardless of format, and is applicable to all staff and stakeholders associated with AQ and data processors acting on behalf of the AQ.

## Aim

The aim of this policy is to standardise AQ's response to any reported data breach incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents, it aims to ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by authorised personnel
- Incidents are recorded and documented
- The impact of incidents is universally understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- External bodies or data subjects are informed as required
- Incidents are dealt with in a timely manner and normal operations restored as soon as possible
- The incidents are reviewed to identify improvements in policies and procedures

# Data Protection Act

All organisations that process personal data must ensure it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).It is the individual responsibility of all who use, keep or collect personal data to apply the provisions of Article 5(f) of the General Data Protection Regulation 2016. It requires that all organisations publish and maintain a policy on data protection which details how personal data is handled. Everyone responsible for using or accessing personal data has to follow strict rules called data protection principles.

They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

AQ also consider enhanced protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Health
- Sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

# AQ staff responsibilities

- AQ staff, associates and 3rd parties who have access to data are responsible for reporting actual, suspected, threatened or potential information security breach incidents and for assisting with investigations as required
- If urgent, action must be taken to prevent further damage

- Managers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required
- The GDPR data team will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan
- Suitable delegation may be appropriate in some circumstances

## Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you.

These include the right to:

- Be informed about how your data is being used
- Access personal data
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of your data
- Data portability (allowing you to get and reuse your data for different services)
- Object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- Automated decision-making processes (without human involvement, such as in remote assessment)
- Profiling, for example to predict your behaviour or interests

## Definition of data breach

GDPR defines a 'personal data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A data breach may occur when for example:

Files:

- Hard copy files or records are left unattended, lost or stolen
- Laptops, iPads, phones, data sticks or any other removable portable device holding personal or sensitive data are lost or stolen
- Databases or case file management systems are accessed by unauthorised users – either accidentally due to inadequate system access controls or intentionally by hackers

- Sharing of learner data to unauthorised third parties

Sensitive or inappropriate information:

- Sensitive information is posted, faxed or emailed to the wrong recipient
- Inappropriate information is released as part of a subject access request
- Data 'blagging' offences where information is obtained by deceit

Equipment and buildings:

- Information is obtained by eavesdropping on phone calls, viewing computer screens in unprotected public spaces e.g., shoulder surfing
- Loss or theft of data or equipment on which data is stored
- Unforeseen circumstances such as a fire or flood damage storage or buildings

Other:

- Unauthorised access to confidential or highly confidential AQ data
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack

This list is not exhaustive and measures should be in place to mitigate different scenarios.

## Cyber security

*'The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. The Regulation does not mandate a specific set of cyber security measures but rather expects you to take 'appropriate' action. In other words, you need to manage risk.'*

https://www.ncsc.gov.uk/information/gdpr

https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Cyber%20strategy&sort=date%2Bdesc

AQ will operate continuous assessment of the risks of cybersecurity risks and keep this and data protection under review. Through the use of encryption and cybersecurity measures we seek to preserve the confidentiality and integrity of personal data.

# Artificial intelligence

AQ remain aware of and monitor the progress and impact of potential risks as new and emerging technologies and generative AI grow. The National Cyber Security Centre (NCSC) publish articles to assist in informing approaches to mitigate risk.
Artificial Intelligence

In relation to final summative AQ assessments, we do not authorise the use of Generative AI and encourage all centres and learners to refer to our *Use of Generative AI Policy*.

# Assessment related data activity

## Recording of assessment

Assessment sessions may be videoed or recorded for marking and quality assurance purposes. No such recordings will be shared wider than for the purpose of AQ internal processes.

AQ will seek to protect the privacy of learners arising from any monitoring, recording and videoing during any assessment. Without being able to record, store or video learners during any live assessment we would not be able to assess you.

## Learner identification

At the start of any recorded assessment session, all learners will be required to show a valid photographic ID and verify their signature using the web camera facility for identification purposes. Sessions will not commence if we are not able to verify a learner's identity.

Furthermore, no learner may be registered for any AQ assessment unless photographic ID is presented at registration.

Accepted forms of photographic ID:

- Passport
- National ID card
- Driving licence

## Learner consent

Showing your photographic ID prior to a recorded assessment taking place will be taken as your consent to being monitored, recorded and filmed for the purposes of your assessment as well as for playback afterwards for marking, quality assurance and for reference in the event of an appeal, complaint or special consideration.

# GDPR Data Controllers and Data Processors

The GDPR draws a distinction between a 'controller' and a 'processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility.

The GDPR defines these terms:

- 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

If you are a controller, you are responsible for complying with the GDPR – you must be able to demonstrate compliance with the data protection principles and take appropriate technical and organisational measures to ensure your responsibilities are carried out in line with the GDPR. If you are a processor, you have more limited compliance responsibilities. AQ have an appointed Controller and Processor.

# Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore, it is important to identify quickly, the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted.

The severity and risk associated with a data breach can be found in *Appendix C: Evaluation of Incident Severity*

# Data Security Breach Reporting

## External identification

Confirmed or suspected data security breaches should be reported promptly to AQ Head of Qualifications by email info@aspirequalifications.com. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process.

Once a data breach has been reported, an initial assessment will be made to establish the severity of the breach and who the responsible officer to lead the investigation should be.

All data security breaches will be centrally logged on the data breach document to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

## Internal identification

As for external identification, internal identification follows the same process with regard to the initial assessment and severity rating. Whether the identification is actual or potential the staff identifier must report it immediately to their line manager who will escalate it to the responsible officer for data.

# Data Breach Management Plan

Each incident of data loss will require a subtly different response plan however, there are four important elements to any breach management plan.

The response to any reported data security breach will involve the following four elements:

- Containment and recovery
- Data sensitivity risk assessment
- Notification/reporting of breach
- Response, evaluation and review

Each of the four elements will need to be conducted in accordance with the following appendices.

Appendix A: Data Breach Management Plan
Appendix B: Data Breach Incident Report Form
Appendix C: Evaluation of Incident Severity and Checklist
Appendix D: Example format of timeline of breach

An example of an activity log spreadsheet is attached (Appendix D)

## References

ICO website: guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

## Policy updating and reviewing

We monitor our policies on an ongoing basis to ensure that they remain fit for purpose and responsive.

All policies relating to AQ will be updated on an 18-month cycle or sooner as required. Earlier policy updates will take place in response to any regulatory change, resulting legislation or feedback received, that dictates the need to conduct an earlier review.

Our policy review process also forms part of AQ's continuous improvement monitoring and self-assessment arrangements.

## Policy version and owner

| | |
|---|---|
| Policy version | October 2024 |
| Policy review date | April 2026 |
| Policy owner | Responsible Officer |
| Regulatory references | Condition A6 – Identification and management of risks<br>Condition A7 – Management of incidents |

# Appendix A: Data Breach Management Plan

**Containment and recovery**

- Relevant key people to be notified and assign severity of the breach using Appendix B
- Forward a copy of the completed data breach form to the allocated organisational investigator
- Investigator to identify the cause of the breach and if it has been contained or if it is ongoing, ensure that any further potential for data loss is either protected, removed or is mitigated as much as possible
- Investigator to determine if anything can be done to recover the loss of data and limit any damage
- Where appropriate they will inform the relevant external authorities
- They will ensure all key actions are logged and decisions/outcomes are recorded

**Assessment of risks**

- What type of data and how much is involved?
- How sensitive is the data?
- What has happened to the data?
- If the data was lost or stolen were there any protections in place to prevent access or misuse e.g. encryption?
- What could the data tell a third party about the individual and how this could be misused?
- Is there actual or potential harm that could come to any individuals?
- Are there wide consequences to consider (media or loss of confidence in AQ)?
- Are there others who might advise of risks (e.g. banks or government authorities)?

**Notification/reporting**

Notification has a clear purpose, it may:

- Enable individuals who may have been affected to take steps to protect themselves
- Ask third parties such as the police, insurers, bank or credit card companies to assist in reducing risks
- Allow the appropriate internal departments to change working practices, perform duties more securely, provide advice and deal with complaints

Questions to ask:

- Are there any legal, contractual or regulatory requirements to notifying?
- Can notification help the individual?

- If a large number of people are affected or there are very serious consequences, inform the ICO
- Consider the dangers of 'over notifying' due to the impact of disproportionate impact
- Consider how you will notify those impacted
    - Consider the urgency of the situation and impact
    - Description of the breach and what data was lost
        - Give specific and clear advice on ways to protect themselves
        - Provide ways individuals can be contact AQ for more information
- Consult ICO guidance on when and how to notify it about breaches
- Consider notifying third parties who can assist or mitigating impact on individuals (police, insurers, banks etc.)

**Review and Response**

- Establish if there are any present or future risks
- Consider the data and context of the breach
- Consider and identify any weak points in existing security measures and procedures, with a view to changing processes or training of AQ staff
- Report on findings and outcomes to Senior management and implement agreed changes

# Appendix B: Data breach incident report form

| | |
|---|---|
| Person initially reporting the breach: (Name, Department, Country) | |
| Time and date breach was identified and by whom: | |
| Description of the Data Breach: | |
| Contact details of person reporting breach: | |
| Type and severity of breach (system and who it affects): | |
| Volume of data involved: | |
| Confirmed or suspected breach: Confirmed: Y/N *Provide further details:* | |
| Is the breach ongoing? | |
| If ongoing, what actions are being taken to resolve the data, mitigate the risk? | |
| Who has been informed of the breach so far? | |
| Has the breach been rectified? Provide details: | |
| Does the Data Breach need reporting to Regulatory Authorities (e.g. Ofqual, ICO)? | |
| Any other relevant information: | |

Please email the completed form to the data team: info@aspirequalifications.com

**For office use only**

| | |
|---|---|
| Received by: | |
| Date/Time: | |

# Appendix C: Evaluation of incident severity and checklist

The severity of the incident will need to be assessed and the relevant members of the AQ team notified, the assessment should be based upon the criteria within the grid:

| Critical level | Main contact |
|---|---|
| Highly Critical: Major Incident | |
| • Highly confidential/Confidential data (including financial information)<br>• Personal identifiable data breach of over 1000 individuals<br>• External third-party data involved<br>• Significant or irreversible consequences<br>• Likely media coverage<br>• Immediate response required regardless of whether it is contained or not<br>• Requires significant response from one or more teams | • A member of the GDPR data team<br>• Chair of Board, CEO, and Manager responsible for the area that has breached<br>• Department Head who is responsible for the area that has breached<br>• Other relevant contacts<br>• ICO or Police |
| Moderately Critical: Serious Incident | |
| • Confidential data<br>• Not contained within AQ<br>• Breach involves personal data of more than 100 individuals but less than 1000<br>• Incident may not yet be contained<br>• Incident does not require immediate response<br>• Incident response may require notification to AQ's CEO | • A member of the GDPR data team<br>• Chair of Board, CEO<br>• Department Head who is responsible for the area that has breached<br>• Other relevant contacts<br>• ICO or Police |
| Low Critical: Minor Incident | |
| • Internal or Confidential Data<br>• Small number of individuals involved<br>• Risk to AQ low<br>• Inconvenience may be suffered by individuals impacted<br>• Loss of data is contained/encrypted<br>• Incident can be responded to during working hours | • A member of the GDPR data team<br>• Department Head who is responsible for the area that has breached<br>• CEO and the Manager responsible for the area that has breached |

# Appendix D: Example format of timeline of breach

**Actual format is a spreadsheet log stored on SharePoint**

| Date | Time | Activity | Decision | Authority | Date Authorised | Escalation details, if required |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |