SUMMIT
Qualifications UK

Data Breach Policy and Process

Scope

Summit Qualifications UK is committed to safeguarding personal data.

This Data Breach Policy explains the responsibilities of Summit Qualifications UK where data security has been breached. The breach is normally some kind of security incident that affects the confidentiality, integrity or availability of data.

Summit Qualifications UK staff, contractors and centre staff must be made aware of, understand and follow this policy.

Whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed this must be advised to Summit Qualifications UK's AO Manager who will report this onto the Data Compliance Officer (DCO).

Data Breach

A data breach may occur where:

- IT systems have been accessed without authorisation
- IT systems or website has been hacked into
- Emails or other communications containing personal data have been sent to an incorrect recipient/s
- Devices holding personal data e.g. laptops, USBs have been lost or stolen
- Personal data has been altered or deleted without an individual's request
- Data has been deleted in error.

Summit Qualifications UK, or a centre where they experience a data breach are required to establish the likelihood and severity of the resulting risk to people's rights and freedoms.

What to do if there is a data breach at a Summit Qualifications UK Centre

Where a centre delivering Summit Qualifications UK qualifications experiences a breach it must notify Summit Qualifications UK of this. The following information should be provided within 24 hours, or sooner:

- The circumstances of the breach
- What the breach constitutes (scope, scale and impact)
- What containment actions have been taken, or will be taken
- Whether the centre has notified the ICO (Information Commissioners Office).
- All third-party suppliers are required to report all security events and data breaches to The Summit Qualifications UK without undue delay and no later than 24 hours after discovery.

Summit Qualifications UK and any centre experiencing a data breach must take steps to detect and investigate the circumstances.

If the breach is likely to impact Summit Qualifications UK systems and data please notify Summit Qualifications UK's AO Manager immediately. Similarly, if a breach is notified to the ICO please advise the Summit Qualifications UK immediately.

Core response - The incident response cycle

The four core response stages are 1) Analyse, 2) Contain, 3) Remediate and 4) Recover

1) Analyse

This stage of the incident involves everything from technical analysis through to a review of social media reactions.

It is important to ensure tasks are prioritised carefully and findings are constantly reviewed and correlated, as these may lead to new tasks. Usually, the initial priority is to understand enough to take containment/ mitigation actions and ultimately remediate the attack.

2) Contain / Mitigate

Once it's safe to do so, we take steps to reduce the impact of the incident and prevent things from getting worse. This usually involves such things as blocking activity, isolating systems and resetting accounts.

This stage may require critical decisions such as taking a core business system offline.

We also evaluate the possibility that the attacker might react to your actions.

3) Remediate / Eradicate

The aim of this stage is to fully remove the threat from the network and systems. This often involves similar actions to containment but is sometimes coordinated so that all actions are carried out simultaneously.

It is important to confirm that remediation has been successful before to moving to the recover stage - this may involve monitoring for a period. Some analysis may continue in this stage too.

4) Recover

At this point, systems are returned to 'business as usual'. Clean systems and data are put back online and in some cases, final actions are taken to handle regulatory, legal, or PR issues.

Throughout the response, all tasks and findings will be tracked. Findings and analyses correlated, response actions re-prioritised.

What Summit Qualifications UK, or its centres must notify to the ICO (Information Commissioners Office)

Depending on the likelihood and severity of the resulting risk to people's rights and freedoms of the breach and if there is a risk then the ICO must be notified.

In assessing the risk Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

As such this means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. The Summit Qualifications UK may also require reporting the breach to Ofqual if there is a potential adverse effect.

If the Summit Qualifications UK or a centre decides not to report the breach to the ICO, it must be able to justify this decision, and so must be documented.

Any breach notifiable to the ICO must be done without delay, or within 72 hours from the point the organisation is aware of it.

Record keeping

Summit Qualifications UK and its centres must keep a record of any personal data breaches, regardless of whether they are reported to the ICO.

Summit Qualifications UK contact

Any data breech must be reported to Summit Qualifications UK's AO Manager.

Any questions on this policy or process should also be directed to the Summit Qualifications UK's Legal Adviser.