Information Security Guidance for Heads of Centres

In the run-up to examinations it is important to consider how centre staff handle electronic data. Electronic records should be treated the same as any other records created as part of the exams process. They must be stored securely within a centre.

With the introduction of GDPR legislation, centre staff must be particularly careful when handling and processing personal information. All entry data will include a candidate's personal data (name, date of birth and address). Candidates with special educational needs may also have sensitive information relating to an access arrangement. It should be noted that candidate consent is required before access arrangements applications can be processed. In addition, information relating to special applications may be equally as sensitive.

Centres receiving electronic examination papers or materials in an electronic format will need to observe the awarding bodies download and security instructions. The storage of internal assessments and transmission of marks to awarding bodies must be undertaken securely to maintain the integrity of the information.

Results will be released electronically to centres on the days before results days. In 2019 these are:

- Wednesday 14 August for GCE A levels, GCE AS levels and Extended Project
- Wednesday 21 August for full and short course GCSEs, Entry Level qualifications and Project

These results **must be kept securely prior to the release of results** and you must follow the JCQ guidance detailed in Release of results June 2019.

Post-Results Services or appeals data must also be kept securely, and a candidate's consent is required before a Post-Results Services request can be processed.

The JCQ Centre Inspection Service give advice on the security and storage of question papers within a centre. However, the security of a centre's IT systems, its internal usage policy and any staff training is the responsibility of the Head of Centre. Any internet enabled IT equipment should have as a minimum:

- up-to-date anti-virus software installed on all devices
- a firewall properly configured for the centre's needs, and
- a well-maintained and up-to-date operating system.

Staff accessing web-based applications or other online systems (including awarding body systems) should be using, where available, a multi-factor authentication password. Password re-use across different applications should be strongly discouraged. Where a centre permits personal use of its IT equipment there must be automatic controls in place to prevent the downloading of malicious software. Staff training should include keeping personal data safe and advice on how to reduce the risk or theft of login credentials.

The NCSC website includes advice to individuals as well as organisations. Some useful links are below.

NCSC – Top tips for staying secure online

The Government minimum standard for cyber security - Cyber Essentials.

More information is available from the National Cyber Security Centre website.

May 2019