Enhancement-led Institutional Review (ELIR) 4 Operational Guidance: Advice for Reviewers on Information Security and Note-keeping[1]

What is in this guidance?

1 The following areas are included:

- details about information security and data protection
- procedure for handling ELIR information while working offline
- keeping notes and related material
- securely destroying notes and materials after the ELIR report is published.

Access to information for reviewers

2 All ELIR reviewers are required to follow the below procedure for working offline when accessing, downloading, creating and storing QAA Scotland (QAAS) information. It is vital that you respect QAA's need to protect the review process and our professional reputation, and to comply with the law. As an ELIR reviewer, you committed to this when signing your contract.

Why this matters

- A review is a confidential process between QAAS and the institution. QAAS relies on institutions being open and honest with us, and institutions rely on QAAS's commitment to keeping both the information they share with us and our judgements about them confidential until the report is published. Breaching this confidentiality could have a detrimental effect on the quality of communications and information sharing between QAAS and institutions, and risk compromising the professional reputation of QAAS and its reviewers.
- If a reviewer were to inadvertently put QAAS information into their own institution's system (for example, by using their work email address to discuss an ongoing review), this information may become subject to the *Freedom of Information (Scotland) Act 2002*.
  As a result, the information can be (and has previously been) requested from the institution by members of the general public. Information released under this Act would then be publicly available.
- If a reviewer were to put QAAS information into a personal cloud-based storage service (such as iCloud, Dropbox, OneDrive), they risk breaching the *Data Protection Act 2018* and compromising the security of commercially confidential information.

[1] Acknowledgement: this paper is based upon similar guidance produced for QAA review visits elsewhere in the UK and has been adapted for the Scottish sector.

- If a reviewer were to comment on the content of an ongoing review on social media they would compromise the confidentiality of the review process and their own professional reputation, as well as risking damage to the institution.
- Where the information that has been compromised is commercially confidential or if the institution suffers from the disclosure, QAAS could face a legal claim for damages.
- Supporting evidence provided as part of the review process sometimes contains personal data relating to staff and students (although QAAS does not require this). If QAAS fails to keep this information secure, we risk breaching the *Data Protection Act 2018* and having to inform the institution, data subjects and the Information Commissioner of the security failure. Fines can be imposed for breaches of the data protection principles, but for QAAS the greatest risk is always to our professional reputation.
- Failure to follow our own procedures or breaching current legislation can form the basis of a legal challenge against QAAS, and therefore it is imperative that QAAS's relevant procedures, processes and guidelines are followed at all times.

If you have any questions concerning this procedure please contact your QAAS officer.

Procedure for working offline

3 QAAS recognises that there will be times when you do not have access to a good internet connection and will need to work offline. To work offline you need to follow the procedure below.

- Password-protect your device.
- Never save your QAAS password into your device.
- Do not put unpublished QAAS information on the web (Dropbox, OneDrive, any app that syncs to cloud-based services).
- Do not put unpublished QAAS information on your work information systems (by sending QAAS review information or attachments through your work
- email, for example).
- Download only what you need.
- Upload the information QAAS needs to the Review Extranet site.
- Inform your review manager if you have any reason to suspect that QAAS's information security is at risk (for example, you lose your device or suspect that your password is compromised).

Private notes

4 Team members should be aware that **any** private notes and **any** communications that they make in relation to an ELIR can be the subject of a Freedom of Information[2] request, or be liable to disclosure in certain proceedings such as judicial review. They may be required to be disclosed in order to show fairness of decision making.

5 In view of this, ELIR team members (and QAAS officers) need to make sure that notes and communications use professional and non-prejudicial language.

[2] There is case history involving a regulatory body which indicates that neither completed evidence forms nor information given in confidence is automatically exempt from disclosure.

6 Legal advice is that any private notes made by ELIR team members should be captured in the official record (see below), and that those private notes should be destroyed at the end of the review, when the report is published.

The official record

7 The only formal and official record of ELIR visit meetings is that kept by the Coordinating Reviewer. This includes both the record of institutional meetings and that of the team's formal private meetings.

8 For institutional meetings, the record consists of notes taken by the Coordinating Reviewer of meetings and the bullet points made afterwards. Coordinating Reviewers copy these documents and distribute them to reviewers and the QAAS officer managing the review. Bullet points capturing the key points from those notes are also posted to the Review Extranet.

9 Copies of all Coordinating Reviewers' notes should be available in a form that is accessible to outside scrutiny should QAAS be called upon to provide them. A photocopy of the notes should be given to the QAAS officer for the official archive, if an electronic copy is not posted to the Review Extranet.

10 ELIR team members are strongly discouraged from making any detailed notes of their own during institutional meetings. Detailed note taking will inhibit full engagement with participants during a meeting. While brief notes may be necessary as an aide-memoire, members should ensure that any of their own notes which they feel need captured are included in the bullet points made after the meeting. This will help to ensure that any observations/findings are shared by the team and are, therefore, based on a collective understanding.

What to do after an ELIR is published

11 Delete all copies of QAAS information when the Outcome and Technical reports are published (this includes all electronic and paper copies), first making sure that you have uploaded into the Review Extranet all information QAAS needs to create a complete and evidence-based record of the review. This includes deleting any notes or annotated documents you may have created during the review. If you have printed documents or hard copy notes, these should also be securely destroyed (by shredding, for example) following publication of the review reports. You must also delete all reviews-related material information from any USB sticks you may have been given by the institution or QAA.