REF 2021:

Technical security user guidance

January 2020

Aim of this guidance

1. In October 2020, the REF development team engaged a third party supplier to undertake penetration testing on the REF 2021 Submission system. One of the outcomes of the exercise was that the REF team should make clear how digital information will be presented and disseminated to the REF community. This will help the user community to be more confident in identifying potentially malicious content purporting to originate from the REF team.

2. This document describes the guidelines for the user community about how the REF team will communicate electronically. It details what the REF team will distribute electronically and what it will not do.

Guidance on electronic communications

3. Emails sent from the REF team will originate only from email addresses from the following domains:
   - **a.** **@ref.ac.uk**
   - **b.** **@re.ukri.org**
   - **c.** **@ref2021.freshdesk.com** (this is the domain used by the user support ticketing system)

   Please ensure that when emails are received that the domain looks correct and matches one of the above.

   Emails from **msonlineservicesteam@microsoftonline.com** will also be sent to users when resetting passwords on the REF2021 Submission system.

4. Hyperlinks in emails will only be used where necessary and will only link to information pages, other than in the following circumstances.

   Exceptions to this are in the following :
   a. Users who have accounts on the support portal hosted by Freshdesk. If a user resets their Freshdesk portal password, they will receive an email containing a URL with a query string to enable them to do so. This will begin with either **https://ref2021.freshdesk.com** or **https://support.ref.ac.uk**.
   b. A link to an existing ticket within Freshdesk for Audit purposes. This link will begin **with either https://ref2021.freshdesk.com** or **https://support.ref.ac.uk.circumstances**

5. Any hyperlinks included in emails will be in full (e.g. https://ref.ac.uk/publications) and not linked from a word or phrase.

6. Users should verify when following links from an email that the destination URL is the address they were expecting to arrive at.

7. REF will never ask for your username/password via email, or over the telephone.

8. Users should never reveal or share their login details.

9. Before logging in to any of the REF systems ensure that the URL is correct:
   a. **https://*.ref.ac.uk**
   b. **https://ref2021.freshdesk.com**

   Ensure that there are no other characters in place of the '.' or any characters missing.

10. The Submission system will always display the time of a user's previous login to the system.

11. If you receive any communication that you are unsure about please contact usersupport@ref.ac.uk to verify its legitimacy.