



Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Advisory Guidelines on European General Data Protection Regulation

Trinity College Dublin, the University of Dublin thanks you for your service to College in your role as an External Examiner.

Following the introduction of the EU – General Data Protection Regulation on the 25th May 2018, we want to alert you that the regulation confers the status of ‘personal data’ on students’ assessed work (exam scripts, coursework, research theses).

External examiners act as ‘data processors’ on behalf of College and all External Examiners whether they be domiciled in the EU or outside the EU are asked to take the steps outlined in this advisory to protect hard copy or electronic copies of students’ assessed work (exam scripts, coursework, research theses) provided to you by Trinity Schools or Departments to facilitate the performance your external examining duties.

This advisory applies:

1. If you receive hard copy documents by registered mail or by courier that you:
 - a. receive the documents in person;
 - b. store the documents securely where they cannot be accessed by unauthorised persons;
 - c. hold onto the documents only for the duration of your examining duties, unless in the case of a research thesis, the student has consented to the examiner retaining a copy of the research thesis beyond the examining period, should they so wish;
 - d. dispose of/destroy the documents through a secure method¹; or return the documents to the School/Department at /upon completion ²of your examining duties, to facilitate their secure disposal by the School or Department.

¹ Costs of shredding and secure disposal may be reimbursed through expenses claim on presentation of receipts.

² Costs of postage for return of documents can be reimbursed through expenses claim on presentation of receipts.



Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

2. If you receive electronic copies through one of Colleges approved platforms that you:
 - a. ensure any passwords received to access, e.g. encrypted files, is stored separately from the documents received, and destroyed once the documents have been accessed successfully or upon completion of your examining duties
 - b. encrypt the files or disc if the documentation is stored on a networked computer to prevent access by unauthorised persons
 - c. not download the documentation to Dropbox or GoogleDocs or any other internet service that can potentially be accessed by unauthorised persons;
 - d. if the files are stored on a local computer ensure that the hard drive is backed up on a regular basis as locally stored data may be irretrievable in the event of a technical issue or the loss or theft of a device if the files/disc are not encrypted.

3. Steps you can take to mitigate the potential of access by authorised persons to files on your computer, include:
 - a. Use the most up-to-date and secure versions of software;
 - b. Use updated virus-protection software;
 - c. Use strong password;
 - d. Do not share your password with anyone;
 - e. Delete files upon completion of your examining duties;
 - f. Empty your deleted files so that documents are permanently deleted.

4. If you suspect your computer or the files have been accessed by an unauthorised person, you are asked to contact the School or the Department at your earliest convenience and within 72 hours of any potential breach having occurred.

We thank you for your co-operation in assisting to ensure compliance with the [EU-GDPR 2018](#).