Newcastle University
General Data Protection Regulation (GDPR)
Brief Update and Guidance

The GDPR will become law across the EU on 25 May 2018 and will be enshrined in a new UK Data Protection Act. It is an evolution of the Data Protection Act 1998 and not revolutionary. It will strengthen the rights of individuals to protect their personal data and increases the sanctions for the misuse of data, including data breaches.

Personal data is information on living individuals who can be identified, directly or indirectly, and relate to either physical, physiological, genetic, mental, economic, cultural or the social identity of the individual. It can be in electronic or paper form. This applies to research data as well as corporate information such as student or staff records.

We must only collect, store and process personal data for lawful purposes, and keep it only for as long as we need it for those purposes. We must not collect excessive or irrelevant information. There are many myths about GDPR. For example, there is a mistaken view that in order to hold <u>any</u> personal data the University must obtain the positive consent of the individual. This is misleading. Consent must be sought if we do not have an alternative lawful basis for processing the data. Where we already have a lawful basis for processing personal data we are not required to obtain new consents.

Alumni records, and what the University does with such information is a notable example where positive consent of individuals must be gained in order for the University to lawfully process such personal information.

Whenever we collect personal data, we must make data subjects aware of the purpose for collecting that data and how to exercise their rights in relation to that data.

Personal data must be kept securely. We should store personal data on encrypted devices. For example, unencrypted memory sticks should not be used to store personal data.

Individuals have a right to see any data we hold on them, including emails that refer to them. We should be mindful of this when writing emails that refer to individuals.

Great care should be taken when attaching spreadsheets, PDFs or similar files containing personal data to emails. If an email is to be sent, we should check the recipients very carefully.

We should consider emailing links to NUIT provided secure, shared file-store for data sharing rather than sending the data via email (thus only those individuals authorised to view that file-store will be capable of reading such data).

Personal data should not normally be transferred outside the University unless there is a legal basis in place to do so. If in doubt, contact the Information Security Team in NUIT.

The 25 May 2018 should not been seen as an end date, GDPR compliance does not stop at that time. The UK Information Commissioner has said of GDPR:

> *It's an evolutionary process for organisations – 25 May 2018 is the date the legislation takes effect but no business stands still. You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018.*

John Hogan
Registrar
31 January 2018