Hello Richard

A few comments made below in green.

Kind regards

Phil

From: Richard Byles
Sent: 20 February 2019 15:50
To: Phil Oakman <Phil.Oakman@northampton.ac.uk>; Robert Farmer <Robert.Farmer@northampton.ac.uk>
Subject: LearnTech blog post on GDPR data '

Hi Phil,

I appreciate you're no doubt very busy, but I wonder if you could spare me five minutes by looking over a draft LearnTech post 'GDPR - considerations for tutors'?

I've copied in Rob F as he's suggested that if it provisionally looks OK, he could take it to the next Data protectors co-ordinators meeting.

All the best.

Richard.

GDPR – Considerations for tutors.

BY RJBYLES ON FEBRUARY 20, 2019 · LEAVE A COMMENT [EDIT]

GDPR – General Data Protection Regulation

The introduction of EU GDPR legislation in 2016 and it's enforcement in May 2018 means that everyone who manages personal data is now responsible for ensuring that it is secure and that data is safeguarded using the highest privacy settings appropriate so that data is not publicly available without a lawfulness of processing criteria identified as required by GDPR Article 6 ~~consent~~. Although our VLE – NILE, is a secure network for students this still law applies and can guide us in how we best go about our day to day duties.

Device security.

When saving data it is best to either use the cloud storage 'OneDrive' or your network drives as locally saved data can be easily hacked should you lose your device. Article 9 of GDPR expects greater degrees of security for sensitive personal data (known as 'special category data') and so any personal information of this sort should also be password protected.

If you are unable to work online and are working on documents which contain student data such as Excel, then you should password protect these. – sensitive personal data should not be worked on offline and snapshots of University databases should never be used to process personal data offline. When users login to NILE it is usually automated due to 'single sign-on' or your password may be held in the browser cache so anyone with access to your computer will be able to login to NILE to view student data. Therefore we ~~suggest~~ strongly advise you do not allow any other users access to your machine, or leave it unattended. When not in use you should always lock the screen (Windows 'CTRL + L' / Mac 'Control + Shift + Power').

If you lose either your work device or a mobile device which is linked to data such as your email, you should report this as a data breach to IT immediately via the UoN Service Desk. so they can secure your account, and the University Data Records Manager Phil Oakman, Phil.Oakman@northampton.ac.uk

Personal Data Breach.

If you become aware of a data breach you should inform the University Data Records Manager Phil Oakman, Phil.Oakman@northampton.ac.uk
Other personal data breaches include:

- access by an unauthorised third party,
- deliberate or accidental action (or inaction) by a controller or processor,
- sending personal data to an incorrect recipient,
- alteration of personal data without permission,
- loss of availability of personal data.
  - Loss of personal data
  - Personal data stolen

Passwords.

Basic passwords can be cracked very easily. This Tech.co article lists some good and bad examples of password

We suggest you don't use your work password for any other sites, as if they are hacked they leave our NILE and IT systems open to hacking, also don't write your password down anywhere or send it on an email.

If you use your smartphone for work, then it is best to choose a longer passcode. A device called 'GrayKey' software is used by government agencies to access iPhones, and can crack a 4 digit security code in a few hours, and a 6 digit code in a few days, but an 8 digit code would take much longer to crack. It is highly likely that hackers use similar software to crack passwords on both IoS and Android, so it is best to increase the number of digits beyond 6.

If you suspect your password is not secure change it here: https://www.northampton.ac.uk/user

Emails

Sending student data by emails is problematic for a couple of reasons; firstly data can be intercepted by email servers, and secondly, it is easy to send an email to the wrong person.

Do not include personal data, and especially sensitive personal data in the body of an email.

To make these more secure you should password protect any files containing student data that you are sending, and send the password in a separate email within an attachment. (not titled 'password')

Revealing grades.

When revealing grades to students, only use the functionality within our VLE – NILE, as this ensures that this private data is only seen by the student to who it applies.

Staff should not use Announcements or Content areas to release grades, or use group names or student numbers to anonymise them – as these are pseudo-anonymous and in breach of GDPR.

Adding group grades to 'Feedback to Learner'.

Any information posted into the 'Feedback to Learner' area in of a Blackboard Group assignment is released to all students in a group, therefore you should not include any grades in this area as this would be in breach of GDPR.

Using student names in announcements or posts.

Using student names to set up groups or perform tasks necessary for facilitating teaching and learning is a 'Legitimate interest' of data. However, staff should be aware that adding additional information such as student numbers, telephone number, address, or age, would be a potential security risk to the students NILE and University account.

Collecting data in collaborative activities,

Tools such as blogs, discussion boards and Padlets are often used for online collaborative activities (such as ice-breakers) in which students' may be asked to share information about themselves. Data such as ethnicity, and sex is recorded in self-portraits and videos, or students may include information such as their home town, or sexual orientation in the written form.

Be particularly cautious of asking students to provide details which are commonly used for (banking) security questions such as; home town, name of pet, mothers maiden name, favourite book and favourite holiday destination.

You may wish to consider whether the activity is a 'legitimate interest' of data as it is linked to the learning of the course, or whether you could redesign the activity to achieve the same learning outcomes without the need for students to provide personal data.

If it is necessary, you may wish to flag up to your students the issues of sharing personal data in a shared digital space. or ask their consent to be 100% GDPR compliant.

Video recordings and virtual classrooms

In the virtual classroom platform Collaborate Ultra, students attending can share their webcams or microphones and post questions in the chat box, this becomes a GDPR issue when sessions are recorded, as all of these are held in recordings.

We recommend that staff either inform the students of the recording prior to the session – including details of where the recording will be made available and to whom. Or make the chat anonymous and remove the ability for students to share their camera and microphone in the session settings.

As it is possible to start and stop the recording during the session staff may choose to anonymise the chat and restrict access to the webcam and microphone during the recorded 'instructional' aspects of the session, then stop recording and make these available for when students are actively participating.

Use of social media platforms.

The University's policy on the use of social media in teaching and learning is that students should not be disadvantaged if they do not wish to sign up to these social media platforms.

The reason for this is that these providers are not licensed by the University and we can not expect our students to sign up to third-party terms and conditions. Therefore staff should only adopt social media tools to share content if all students can view the content without signing up for an account, examples of these are Twitter and Instagram.

If the use of Social Media is a learning outcome for a module, the course leader will need to make all potenial students aware of this prior to enrolling on the course through a declaration on the course information page within the university website.

For the same reason, staff should not ask students to use social media platforms (such as FaceBook or WhatsApp) for class communications. There are already tools in the group settings within the VLE to do this such as discussion boards, blogs, email or Collaborate (groups)

Third Party Tools

There are many very useful online tools such as Socrative, Kahoot and Prezi which are commonly used for teaching and learning but are not supported by Learning Technology. In a similar way to the University's policy on social media accounts, the University policy says that students should not be disadvantaged if they do not wish to sign up to third party tools. Therefore staff should either only use tools allow students to partipate without setting up an account, or provides a supported alternative which does not prejudice the student.

Personal student data with third-party publishers.

Third party content providers may require students to sign up to accounts to access their platforms. If this is the case students should be made aware of this prior to enrolling on the course through a declaration on the course information page within the university website.

Sharing student data in research.

If you are sharing student data in your research you will need to make it fully anonymous, and ensure there is no way to link back to the individual it relates to, in practice this may mean that you do not identify module codes. You should also create a Data Management Plan (DMP). For more information contact our Head of Research Support. – Dawn.Hibbert@northampton.ac.uk

Richard Byles
UoN Learning Technologist
Library & Learning Services