LIVERPOOL HOPE UNIVERSITY

LIVERPOOL HOPE UNIVERSITY

INTRODUCTION TO WORKING FROM HOME AND GDPR

Due to the outbreak of Coronavirus, most employees of the University are now working from home. Although this may change some aspects of your job role, it is still important that you continue to comply with GDPR. You may be required to deal with personal data whilst working from home. You need to ensure that the data you are accessing is necessary and that it is secure.

This note contains a few hints and tips to help you with continued compliance.

Important Links

If you haven't already completed the online GDPR training please could you do so now. This training is mandatory for all staff dealing with personal data. Even if you have previously completed the training, a refresher is advised. If you have any questions regarding this training, please contact Shauna Anton.

Please ensure that at the end of each day, you upload the documents you have worked on / created onto the appropriate University network drive (I Drive for personal files; Z drive for Shared files using the FILR facility and then deleting the documents from your local drive. Using this facility will assist with the security of University data and ensure that files are backed up.

Take a look at the University Data Protection Policy, Portable Data Device Security Policy and Information Management Policy to refresh your understanding of your responsibilities in relation to managing and processing personal data.

If you think there has been a breach of GDPR eg. you become aware that data has been lost, you have suffered some sort of cyber-attack or sent an email to the wrong recipient then please follow the Data Breach Procedure.

There are more resources and information about GDPR available at
https://www.hope.ac.uk/aboutus/governance/generaldataprotectionregulations/

https://ico.org.uk/

LIVERPOOL HOPE UNIVERSITY

GDPR GUIDELINES WHEN WORKING FROM HOME
DOS AND DON'TS

DO take care to ensure that when data is no longer required it is deleted from your local device. This includes any files that have been saved automatically as part of the download process.

DON'T send any documents that contain data without using password protection, encryption or pseudonymization.

DO make sure you fully close down all applications that you have been using and then disconnect from the remote connection if established

DO ensure your home Wi-Fi / Broadband is password protected and the home router admin password is not using the original default setting

DON'T store personal data on your own personal devices or on USB sticks.

DO change your password regularly and make it memorable, unique and unidentifiable in line with the University password policy

DON'T send any documents containing personal information to / from your personal email address - only use your Hope account.

DO ensure you have a firewall, anti – virus and anti- malware software and that they are always up to date.

DON'T leave data unattended.

DO report any breach/ loss of personal data immediately to ITSHELP@hope.ac.uk with the subject header: DATA BREACH. The University only has 72 hours to notify the Information Commissioner's Office.

DON'T throw any papers containing personal data in your normal waste. Keep this information locked away until you can return to the office and dispose of it correctly.

DON'T allow your screen to be visible to anyone else, where possible.

DO ensure your windows and doors are locked and your PC / laptop/tablet is out of sight.

DON'T write down any usernames or passwords

DO ensure your laptop/pc is password protected. When you are away from your laptop, ensure your laptop/pc is locked (Ctrl, Alt + Del)

DON'T open any file until you are certain that it is from a genuine source