LIVERPOOL HOPE UNIVERSITY
1844

LIVERPOOL HOPE UNIVERSITY

THE GENERAL DATA PROTECTION REGULATIONS – DOS AND DON'TS

DON'T use data for any reason other than what it was originally collected for.

DON'T leave data unattended. Keep a clear desk, tidy confidential data away when not in use.

DO consider whether it's necessary to use personal data to achieve your objective.

DON'T collect or allow others to access personal data 'just in case'. Collect or use the minimum amount of personal data as needed for your specific objective.

DO Ensure that data is accurate and up to date. For this aim use centralised sources of data where possible, this will also avoid creating unnecessary copies of the same information.

DO Anonymise or pseudonimise data where possible.

DON'T keep data for longer than is necessary. Do regularly and securely destroy out of date information and data that is no longer required in paper form or electronic records. Check what the retention period is for the data you're storing.

DO encrypt attachments or password protect large volumes or special category data if sending electronically.

DO make sure you have the sender's permission to share/forward their name or address when using email or use the blind copy function so recipients can't identify each other.

DON'T write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. You must assume that anything that you write about a person will be seen by that person.

DON'T share data with other teams or departments unless there is a genuine business need to access personal data. Establish a way to share data securely.

DON'T share personal data with external agencies or third parties (eg parents) unless you are sure that there is a legal basis for doing so.

DON'T store personal data on your own personal devices or on USB sticks. DO use secure areas provided by the University for working on and storing personal data.

DON'T use cloud based systems to store personal data, unless security controls for that system have been reviewed by IT Services.

DO be particularly careful when dealing with special category data: eg data concerning race or ethnic origin, political opinion, religious belief, sexual life, criminal offences, trade union membership, health.

DO report any breach/loss of personal data to the Head of Legal Services, Governance and Risk immediately. The University only has 72 hours to notify the Information Commissioner's Office.

DO take time to complete the University training on Data Protection and access the Staff Guidance Book at http://www.hope.ac.uk/aboutus/governance/dataprotection/