

DO:

- ✓ Be organised when it comes to personal data collection.
- ✓ Only collect personal data that is necessary to achieve your purpose.
- ✓ Ensure that you have a lawful basis for collecting personal data.
- ✓ Where you need to obtain the consent of a data subject to collect and process their personal data, that consent should be explicitly made.
- ✓ Ensure that you have informed the data subject of your reasons for collecting their personal data and of their data protection rights by way of a privacy notice.
- ✓ Consider whether you should complete a data protection impact assessment in cases where your research or project may have a high risk impact on the subject's personal data.
- ✓ Safeguard the confidentiality of all personal data you have contact with.
- ✓ Create a permissions structure to prevent misuse or unauthorised/improper access to personal data.
- ✓ Anonymise personal data where possible.
- ✓ Ensure that access to personal data is on a need to know basis.
- ✓ Ensure that you cannot be overheard when discussing an individual's confidential data.
- ✓ Ensure that personal data are kept secure and that portable records are kept in recognised filing/storage places that are locked when access is not directly controlled/ supervised.
- ✓ Check that you are not keeping personal data any longer than is necessary and keep to retention and destruction timeframes.
- ✓ Verify the identity of any person making a request for personal data and ensure they have a need to know.
- ✓ Contact the Data Protection Officer at legalservices@soton.ac.uk if you need to share personal data without consent.
- ✓ Set boundaries for the secure sharing of personal data.
- ✓ When it is necessary, transfer personal data securely and only to those who have a legitimate interest in accessing that data.
- ✓ Ensure that appropriate data sharing agreements are in place before you share data.



Report any actual or suspected breaches of confidentiality or privacy.



Participate in induction, training and awareness raising sessions on privacy issues.



Build in retention/deletion rules based on your classification scheme.



Ensure that personal data is disposed of appropriately as confidential waste.



Put computers into a password-protected mode, if you leave your desk for any length of time.



Keep personal data safe online. Please familiarise yourself with the University's [security tips](#).



Remember that the University will never ask for your password in any communication or email.



Contact infosec@soton.ac.uk on "Privacy by Design" or other systems, information or processes design work.

DON'T:



Share passwords or leave them lying around for others to see.



Use personal data unless absolutely necessary. Consider using anonymised data instead or pseudonymised data (from which direct identifiers have been removed) instead.



Collect, hold or process more data than you need for your purpose.



Transfer data internally for different purposes or externally without any lawful justification.



Keep personal data for any longer than necessary for the purpose(s) it was collected.