Information Assurance Office

Understanding Special Category

The Data Protection Act 2018 (DPA) is based around seven principles of 'good information handling'. These principles give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. If we hold information about individuals either on computer, in a manual form such as paper or in certain types of filing system, we may be holding 'personal data.' How and why we hold and use this personal data determines if UEL is following the Data Protection Act. Some personal data is particularly sensitive. In such cases, it is called 'Special Category' data. Special Category data needs more protection and examples would include information about someone's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This type of data needs additional protection because if it was lost, disclosed in error, or destroyed by accident could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Handling Special Category Data

Because of the increased risks associated with handling Special category data, it is important that it be handled with care and consideration. Key things to bear on mind are:

- Special Category Data must only be used if UEL can demonstrate it has a legal reason to use and process it
- It must be limited to the minimum necessary for us to do what we need to do with it
- It must be kept secure
- It must only be shared when necessary
- It should only be collected when someone understands why it is necessary

Keeping Special Category Data Secure

Using good security practices can significantly reduce the risk of something going wrong such as losing data or disclosing it in error. Simple measures vastly reduce the risks:

- Lock away paper with lots of personal data when your away from your desk or its unattended
- If your sharing a file internally send it via OneDrive for Business or SharePoint rather than email attachment
- If sharing externally make sure to double check the recipient of the data and consider password protecting the file
- If you have used data for its purpose and don't need the raw data anymore, get rid of it
- Don't keep unnecessary duplicates
- Don't store UEL data outside of UEL network e.g. on Dropbox or Google Drive