What will stay the same	What will be new	What does this mean for me
Principles Most of these will remain the same as the Data Protection Act (DPA) 1998: – lawfulness, fairness and transparency – purpose limitation – data minimisation (adequate, relevant and limited to what is necessary) – accuracy – security	Under GDPR, there is a new accountability principle, which means we must be **able to demonstrate** compliance with the principles. In practice this means all uses of personal data need to be recorded in asset registers. These registers should include: – the purpose – the legal basis for processing – the retention period	Ensure that you understand the existing data protection principles. Ensure you can demonstrate compliance by: – Documenting your workflows – Ensuring you have a legal basis for processing, e.g. consent – Ensuring that you have an information asset register in place and it is up to date – Ensuring that you or your office have completed the Annual Data Holdings Survey
Personal data - the definition in DPA 1998 and GDPR is similar.	Includes online identifiers, location data and online identifiers. Here is the full definition: *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'*	This means that almost any activity you perform relating to an individual will probably fall within scope of the GDPR. If in doubt about whether it is personal data or not, err on the side of caution and assume that it is and that the GDPR applies.
Codes of conduct The ICO has published a series of Codes of Conduct to help organisations comply with data protection legislation, and these remain useful and relevant guidance: – Anonymisation – Audits – CCTV – Data processing – Data sharing – Employment – Encryption	No new Codes have been published for the GDPR yet.	Staff are encouraged to follow the existing ICO's codes of conduct opposite where they are relevant to their work, as this guidance offers a solid basis for compliance with GDPR.

– Marketing – Personal data online – Privacy by design – Privacy notices – Security – Subject access		
Consent Consent still forms an important part of data protection, but the definition has changed under GDPR.	Under GDPR consent means: *'…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed.'*	This means that use of 'opt outs' or pre-ticked boxes are no longer an acceptable way to ensure consent. Ensure that any processing you are doing using consent meets this higher threshold.
Sensitive personal data categories remain the same, e.g. information on an individual's: – racial or ethnic origins – political opinions – religious or philosophical beliefs – trade union membership – health – sexual life – offences	Under GDPR sensitive personal data is now caller **special category personal data** and has been expanded to also include: – genetic – biometric personal data	Make sure you are aware of this wider definition and only process it accordingly. Check that you have a condition for processing this special category personal data, e.g. http://www.privacy-regulation.eu/en/9.htm
Breach notification - this has been voluntary under the DPA1998, but the GDPR makes this mandatory.	There is a new obligation to report breaches of personal data security to the ICO within 72 hours.	This means that all staff members must report personal data breaches immediately, in accordance with this procedure. Ensure that you and your team are familiar with it.
Security – the obligation for us to protect personal data remains, but it is enhanced under GDPR.	An obligation to encrypt high risk personal data and use pseudonymisation techniques to minimise exposure. All staff that handle personal data must take the data protection and information security training.	'If large quantities (more than 20 records) of personal information or sensitive personal data are transferred off UCL servers, then it should be encrypted using our guidance. Ensure you have taken the information compliance training - DP, FOI and Security
Fair Processing Notices (FPNs) – these are 'privacy notices' that you often see on forms, sometimes called 'collections texts' or	Under the GDPR, the requirements for FPNs have been expanded considerably to include things like:	If you collect personal data, ensure that your FPNs meet the new requirements in 13/14 of the GDPR.

'small print'. They are a key part of ensuring that processing is fair.	– legal basis of processing – retention periods – recipients of personal data – purposes for processing – rights for individuals A full FPN requirement list can be found in Article 13 and 14 of the GDPR.	If you collect personal data and this processing is not covered by a privacy notice, UCL will breach the *lawfulness, fairness and transparency* principle.
Data protection by design and default	Data protection by design and default is a new approach to privacy that encourages consideration of data protection at an early stage of development.	Ensure that for new projects and systems, you can demonstrate that you have integrated data protection into your processing activities, e.g. use of privacy impact assessments (see below) and the ICO's guidance.
Privacy Impact Assessment (PIA) – this is good practice under DPA 1998, but not mandatory.	Under GDPR, PIAs are mandatory for high risk processing on a large scale or for new projects	Staff responsible for systems or processing that is high risk or large scale, e.g. CCTV, must undertake a PIA. For researchers, consideration of PIAs is now part of the data protection registration process.
Subject access – individuals are entitled to access the personal data we hold on them.	The time for response has been reduced to 30 days.	Ensure you know about this right. Be professional in what you record, particularly in your emails as staff you write about may have the right of access to them
Data portability	Under GDPR, data portability gives individuals the right to ask for their personal data to be provided to them in a commonly used and machine-readable format so they can reuse in other products and services. It only applies to personal data that has been provided by the individual under contract or under consent. This is different to the right of subject access.	Check whether this applies to your work, as the right only applies: – to personal data an individual has provided to UCL; – where processing is based on consent or for the performance of a contract; and – when processing is carried out by automated means. If it does apply, then consider how you would meet requests.
Rectification	Rectification - individuals are entitled to have personal data rectified if it is inaccurate or incomplete within a month.	Ensure that you can administer changes to personal data that is held on request.

Right to erasure (to be forgotten (RTBF) – this provision only applies under DPA 1998 if there is substantial damage or distress to an individual. With such a high threshold it was rarely used.	Under GDPR, RTBF is a much broader right that allows individuals to request the deletion or removal of personal data in certain circumstances without concern for the threshold of damage or distress.	Consider how this right applies to the personal data you hold.
Other individual rights	Other rights: – right to be informed – automated decision making, including profiling – restricting processing	Check to see if any of these rights apply to your work and the personal data that you hold by checking the ICO's guidance.
Data Protection Officer (DPO) Little formal responsibility under the DPA 1998	Under GDPR, a DPO is mandatory for UCL as a public authority and is given a much wider role, including: – to inform and advise of their data protection obligations – to monitor compliance with the GDPR – to provide advice on PIAs – to cooperate with the ICO	Consult where necessary.
Contracts with processors and contractors These were a requirement in the DPA 1998, but have been expanded under GDPR	Under GDPR, agreements containing data protection clauses will need to be updated.	Central guidance is being prepared, please prepare for contracts to be updated to GDPR standards.