Appendix 2: GDPR Principles (DPA 2018)

The GDPR sets out seven key principles:

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

The first principle is relatively self-evident: organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects. To remain lawful, you need to have a thorough understanding of the GDPR and its rules for data collection. To remain transparent with data subjects, you should state in your privacy policy the type of data you collect and the reason you're collecting it.

2. PURPOSE LIMITATION

Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose. Processing that's done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom.

3. DATA MINIMISATION

Organisations must only process the personal data that they need to achieve its processing purposes. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimisation makes it easier to keep data accurate and up to date.

4. ACCURACY

The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

5. STORAGE LIMITATION

Similarly, organisations need to delete personal data when it's no longer necessary. How do you know when information is no longer necessary? Lambeth has a Record Management and Retention policy and Retention schedule that need to be adhered to.

6. INTEGRITY AND CONFIDENTIALITY

This is the only principle that deals explicitly with security. GDPR states that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". The GDPR is deliberately vague about what measures organisations should take, because technological and organisational best practices are constantly changing. Currently, organisations should encrypt and/or pseudonymise personal data wherever possible, but they should also consider whatever other options are suitable.

7. ACCOUNTABILITY

Accountability is one of the data protection principles - it makes the organisation responsible for complying with the GDPR and says that you must be able to demonstrate your compliance. The organisation needs to put in place appropriate technical and organisational measures to meet the requirements of accountability. There are several measures that an organisation can, and in some cases must, take including:

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on your behalf;
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer; and
- adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing. An organisation must review and, where necessary, update the measures you put in place. If an organisation implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation. Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.