

Netherton Park Community Association

The General Data Protection Regulation (GDPR) Summary

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which determines how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

'Personal data' means information that can identify a living individual.

The regulation will apply even after the UK leaves the EU and covers the operation and governance of Netherton Park Community Association (NPCA). NPCA is registered with the Information Commissioner's Office.

Main principles

The GDPR sets out the key principles that all personal data must be processed in line with.

Data must be:

processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also stronger rights for individuals regarding their own data.

The individual's rights include:

to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

New requirements

The GDPR is similar to the Data Protection Act (DPA) 1998 (which NPVA complied with), but strengthens many of the DPA's principles. The main changes are:

- Organisations must appoint a data protection officer, who will advise on compliance with the GDPR and other relevant data protection law
- Privacy notices must be in clear and plain language and include some extra information – the charity's 'legal basis' for processing, the individual's rights in relation to their own data
- Charities will only have a month to comply with subject access requests, and in most cases can't charge this condition
- Where NPCA needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous
- There are new, special protections for children's data
- The Information Commissioner's Office must be notified within 72 hours of a data breach
- Organisations will have to demonstrate how they comply with the new law
- Higher fines for data breaches – up to 20 million euros

A copy of Netherton Park Community Association's GDPR Policy and procedures is available on request.