DATA PROTECTION POLICY

V1.0

ADOPTED 23rd NOVEMBER 2026

AYTHORPE RODING PARISH COUNCIL DATA PROTECTION POLICY

Contents

Introduction	3
Definitions	3
Data processing – the six principles	4
Paper files and manual records	6
Rights of data subjects	6
Registration	7
Exemptions	7
Penalties	8
How does the 2018 Act affect local councils?	8
Manual records	9
Computerised records	9
Data protection complaints handling	10
Further information	10

Introduction

The Data Protection Act 2018 (the 2018 Act) gives effect in UK Law to the General Data Protection Regulation (GDPR). It provides the statutory framework for the use of computerised information (including microfiche, audio and visual systems) and also certain manual records about living identifiable individuals in the United Kingdom. Data Protection legislation does not prohibit disclosures of such information to third parties, but it regulates the circumstances in which they can be made. It gives enhanced "subject access rights" and created a new category of "sensitive data". It also prohibits the transfer of personal data to countries which do not have an "adequate level of protection". Annex 1 summarises in table form the relevant GDPR requirements.

Definitions

The 2018 Act again creates its own definitions, which can be found in Annex Two below. The important definitions are:

- "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "Data subject" means the identified or identifiable living individual to whom personal data relates.
- "Personal data" means any information relating to an identified or identifiable living individual.
- "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:
    - An identifier such as a name, an identification number, location data or an online identifier.
    - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- "Processing", in relation to information, means an operation or set of operations which is performed on information or on sets of information, such as:
    - Collection, recording, organisation, structuring or storage.
    - Adaptation or alteration.
    - Retrieval, consultation or use.
    - Disclosure by transmission, dissemination or otherwise making available.
    - Alignment or combination.
    - Restriction, erasure or destruction.
- "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Processing – The Six Principles

Those who decide how and why personal data is processed (data controllers) must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection legislation.

Anyone processing personal data must comply with the six enforceable principles of good practice. They say that personal data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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 legislation requires that personal data be processed "fairly, lawfully and in a transparent manner". Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject is also entitled to know the identity of the data controller and why information is, or is to be, processed.

"Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:

- Collection, recording, organisation, structuring or storage.
- Adaptation or alteration.
- Retrieval, consultation or use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure or destruction.

Processing may only be carried out where one of the following conditions has been met:

- Consent — The individual has given clear and explicit consent for you to process their personal data for a specific purpose.
- Contract — The processing is necessary for a contract you have with the individual or because they have asked you to take specific steps before entering into a contract.

- Legal obligation — The processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests — The processing is necessary to protect someone's life.
- Public task — The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests — The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. It is not enough to simply say: "We have a legitimate interest in processing allotment holder data", as this does not clarify your purpose or intended outcome. Instead, you need to be more specific about your purpose, such as: "We have a legitimate interest in ensuring that the allotments are used with the terms of the tenancy and the council's allotment rules".

In our opinion, local councils will be able to rely on several of these conditions in ensuring they comply with the 2018 Act.

Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Sensitive data can only be processed where:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest.

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, for medical diagnosis, the provision of health or social care or treatment or for the management of health or social care systems and services.
- Processing is necessary for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Paper files and manual records

GDPR applies to "information kept on paper" if the paper records are kept within a "filing system." The term "filing system" is defined as "any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed..." As a result, any files that "are not structured according to specific criteria" do not fall within the scope of the regulation.

Rights of data subjects

A person about whom information is held (a data subject) is, subject to any exemptions applying, entitled to:

- Be informed by any "data controller" whether any information is held on them together with:
  - A description of the data.
  - A copy of the information in an intelligible form.
- Request and receive information giving:
  - The purposes for which the data is being held.
  - The recipients or classes of recipients to whom it may be disclosed.
  - The source of the data.
- Restrict the processing of their data.
- Object to the processing of personal data for direct marketing purposes (including profiling to the extent that it is related to direct marketing).
- Not to be subject to automated decision-making.
- Receive compensation from the data controller and/or the data processor for the damage suffered as a result of an infringement of GDPR.
- Obtain from a data controller without undue delay the rectification of inaccurate personal data.
- Erase personal data (also known as the "right to be forgotten"), which means that data subjects will be able to request that their personal data be erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed,

where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with GDPR. However, the further retention of such data will be lawful in some cases, e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims. Where the data controller has made the personal data public and is obliged to erase the personal data, it shall take reasonable steps to inform data controllers who are processing the personal data that the data subject has requested them to erase any links to or copy or replication of that personal data.

- Be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights.
- Receive a copy of personal data or to transfer personal data to another data controller (data portability).

Access to personal data held by a data controller must be dealt with within one month of the request and free of charge. Where requests are manifestly unfounded or excessive, in particular, because they are repetitive, the data controller may charge a fee for providing the information or refuse to respond.

Registration

Under GDPR, there is no requirement for a data controller to register with the ICO. However, the Data Protection (Charges and Information) Regulations 2018 (the 2018 Regulations) require data controllers to pay a data protection fee to the Information Commissioner's Office (ICO) unless they are exempt from payment. Councils in England and Wales and parish meetings are public authorities for the purposes of the 2018 Regulations, and they are data controllers.

Data controllers will pay different fees depending on the number of staff and turnover. The ICO has **guidance** on its website.

Members of staff include employees, other workers and office holders. Each part-time staff member is counted as one member of staff.

Non-payment or incorrect payment of the data protection fee could result in a fine of £4,350.

Councillors who are data controllers independent of their council (e.g. constituency casework or election canvassing) will be required to pay the data protection fee.

Exemptions

Data Protection legislation exemptions from obligations and individual rights include:

- National security.
- Defence.
- Public security.
- The prevention, investigation, detection or prosecution of criminal offences.

- Other important public interests, in particular, economic or financial interests, including budgetary and taxation matters, public health and security.
- The protection of judicial independence and proceedings.
- Breaches of ethics in regulated professions.
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention.
- The protection of the individual, or the rights and freedoms of others.
- The enforcement of civil law matters.

Also exempt are:

- Manual unstructured data held by public authorities, which includes local councils (e.g. loose pieces of paper not held in a structured format).
- Manual unstructured data used in longstanding historical research.

Penalties

If the ICO is satisfied that a data controller has breached the legislation, it is open to that Office to serve an enforcement notice requiring compliance. Failure to comply with such a notice can be a criminal offence punishable with a fine.

In addition, the court and ICO have power to award compensation to data subjects who suffer damage and distress as a result of any contravention by a data controller of any of the requirements of the 2018 Act.

How does the 2018 Act affect local councils?

There are exemptions to the requirements and individual rights. NALC takes the view that local councils will be hard-pressed to argue that all their data processing falls within the scope of those exemptions. In short, this is because local councils (like all local authorities) hold such a wide range of information.

It is clear that councils are affected by the provisions of the Data Protection legislation in a multitude of ways. “Personal data” may be as simple as holding someone's name and address but in addition includes, amongst other things, details of complaints, lists of contacts, employee/personnel records and information provided for the purpose of placing a contract to which the data subject is a party. Images taken by CCTV systems also fall within the data protection regime.

The following are a number of practical considerations which a council may wish to bear in mind to help ensure it complies with the 2018 Act:

- A council should first look at any data it holds to see if it includes personal data. Particular attention should be given to such things as contractor/supplier lists where there are businesses involved, as they could contain personal data, as many businesses are owned by sole traders or partnerships. Even with companies, a council may store personal data on contacts at the company.

- It should be noted the legislation only applies to the "processing" of personal data, but processing is so widely defined it will in fact catch almost any conceivable operation on such data.
- A council should (if appropriate) consider where it obtained any personal data from. Unless it can prove it was obtained fairly, there is a risk the law will be broken. What constitutes “fairly” is somewhat complex, but it includes the data subject consenting to the council using it, e.g. was the data subject originally told their data might be given to third parties?
- A council should ensure that individuals are aware of the uses that will be made of the information they supply and, where necessary, give their consent to that specific use. Where there is a legitimate interest or a legal requirement, then consent need not be explicitly obtained. Otherwise, explicit consent must be obtained.
- Data should never be given (or sold) to anyone else unless the data subject has given his/her consent or there is, by law, a duty to do so. Use of personal data on a website will automatically be a breach of the legislation unless express consent has been given, e.g. publishing staff names and mobile numbers.
- A council obtaining consent to any use should make sure that it is "informed consent", i.e. that it is made very clear exactly what the council intends using the data for and what data it is holding.
- A council should ensure it only keeps the bare minimum amount of information necessary for its purposes. It should carry out regular reviews to check that all of the information asked for on, for example, application forms or registration forms really is necessary.
- All data recorded must be accurate, kept up-to-date and deleted when no longer required.
- The information must be kept safe and secure at all times. The level of security will depend upon the sensitivity of the data involved.

Manual records

Filing cabinets need to be locked outside of normal working hours, and keys must be held securely by nominated staff. It is advisable for more than one person to hold the keys, e.g. clerk and ~~another staff member or~~ a councillor. All papers should be securely locked away when not in use to prevent other people from inadvertently gaining access. Councils should have processes in place for homeworkers and information security.

Computerised records

The following guidelines apply:

- Access should be controlled by a unique password, and passwords should be changed on a regular basis. Passwords should not be obvious.
- Passwords and access controls should be kept secure when not in use, e.g. passwords should not be written down and attached to PCs.

- Personal information should not be left displayed on the screen when not in use – councils should consider setting up screens to automatically lock after a certain period, e.g. four minutes.
- Removable devices such as USB sticks should be filed away securely and not left lying around.
- Computers should be turned off when not in use.
- If the personal data is held on a laptop or tablet, these should be securely stored when not in use and be password protected.
- Workspaces containing a computer or other device containing data should be locked when not in use.

Data protection complaints handling

As of June 2026, councils must have a process in place for handling data protection complaints.

Further **guidance** is available.

Further information

The regulatory body with responsibility for enforcing the legislation's requirements and promoting compliance and good practice is the ICO. The relevant contact details are:

- Address — Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
- Helpline — 0303 123 1113
- **Website** (includes live chat option)

The ICO provides advice and publishes useful guidance on data protection legislation. Councils can also contact the ICO with non-legal queries.