

Data Protection Policy

RPC Telecommunications Limited

Last updated	28 October 2026
--------------	-----------------

Definitions

Company	means RPC Telecommunications Limited.
UK GDPR	means the UK General Data Protection Regulation, as amended (including by the Data (Use and Access) Act 2025), which is read together with the Data Protection Act 2018.
Responsible Person	means Mark Charles John Posen, Managing Director.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Company.

1. Data protection principles

The Company is committed to processing data in accordance with its responsibilities under the UK GDPR and the Data Protection Act 2018.

Article 5 of the UK GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and
- f. 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.

2. General provisions

- a. This policy applies to all personal data processed by the Company.
- b. The Responsible Person shall take responsibility for the Company's ongoing compliance with this policy.
- c. The Company shall be responsible for, and be able to demonstrate, compliance with the principles in section 1 (the accountability principle).
- d. This policy shall be reviewed at least annually, and whenever there is a material change in data protection law or ICO guidance.
- e. The Company shall pay the annual data protection fee to the Information Commissioner's Office (ICO) unless an exemption applies, and the Responsible Person shall ensure that it is renewed on time.

3. Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of Systems.
- b. The Register of Systems shall be reviewed at least annually.
- c. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with within the statutory time limit, with reasonable and proportionate searches made for the personal data requested. The Company shall also respect the other rights of individuals under the UK GDPR, including rectification, erasure and objection.

4. Lawful purposes

- a. All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).
- b. The Company shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's systems.

5. Data minimisation

- a. The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

- a. The Company shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, the Company shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why, and the resulting retention periods shall be recorded in a retention schedule kept with the Register of Systems.
- c. Where it is not practical to review and archive personal data (e.g. for emails) these may be retained indefinitely or until such time as deleted by the user. However, the Company shall ensure that any data so retained continues to be subject to the Security provision, and all other relevant provisions, of this Data Protection Policy.

8. Security

- a. The Company shall ensure that personal data is stored securely using modern software that is kept up-to-date.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable (it is noted that some external systems may in the normal course of their operations maintain a recovery window during which deleted data may be restored; however following the end of that period, deleted data shall be irrecoverable).
- d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](#)).

Any member of personnel who becomes aware of an actual or suspected personal data breach shall report it to the Responsible Person immediately.

Where a breach is likely to result in a risk to people's rights and freedoms, the Company shall report it to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it, even if not all of the details are yet available.

Where a breach is likely to result in a high risk to individuals, the Company shall also inform the affected individuals without undue delay.

The Company shall keep a record of every personal data breach, whether or not it is reported, including the facts, its effects, the action taken and the reasons for any decision not to report it to the ICO.

10. Complaints

Individuals who believe the Company has infringed their data protection rights may complain to the Company. Complaints may be made in any form, including by email or in writing to the Responsible Person, and do not need to refer to legislation.

The Company shall acknowledge and investigate each complaint, and tell the complainant the outcome, within the time limits required by data protection law. Complaints shall be recorded and coordinated with the handling of any related data subject access or other rights request.

The Company's privacy notices and responses to individuals' requests shall explain how to make a complaint to the Company and tell individuals of their right to complain to the ICO.

END OF POLICY

Review status

<i>6 August 2018</i>	<i>Policy initially developed and adopted</i>
<i>6 August 2019</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>6 August 2020</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>27 July 2021</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>29 July 2022</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>04 August 2023</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>01 August 2024</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>05 August 2025</i>	<i>Policy reviewed; re-adopted without changes</i>
<i>28 October 2026</i>	<i>Policy reviewed; amended to reflect the UK GDPR, the Data (Use and Access) Act 2025 and ICO guidance, including new complaints, breach-handling and ICO fee provisions</i>

Next review: **No later than 28 October 2027**