

DATA PROTECTION AND GDPR POLICY

AREAS OF APPLICABILITY

This policy applies to the holding and use of personal information (e.g. name, contact details, personal characteristics).

EXAMPLES OF APPLICABILITY TO ABBEY LINE CRP ACTIVITIES

Some examples of activities that this policy is applicable to are listed below, but it should be noted that there will be other activities covered by the policy:

- Database of contact details
- E-mail communications
- Image consent forms

POLICY

Compliance with GDPR

The Abbey Line Community Rail Partnership will adhere to the principles set out in the General Data Protection Regulation (GDPR):

- 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 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.

Data Controller

The CRP Officer is nominated as the Data Controller, and has the responsibility for ensuring that everyone who acts on behalf of ALCRP is aware of the data protection rules.

Data Audit

The CRP will maintain a record of all databases that it holds that contain personal information. Databases include, but are not limited to, computer files, written records and contact lists on mobile phones.

The record of databases will be reviewed at least annually.

Databases

All reasonable efforts will be undertaken to ensure that access to databases containing personal information will only be available to those undertaking authorised ALCRP activities. This will include password protection on computer files and ensuring that any written files are stored in a locked facility.

Information that is out of date or no longer required will be destroyed.

Opt-In

Provision will be made so that people actively opt-in to the storage of their personal data. ALCRP will not store any personal data where the opt-in has not been received.

The use which will be made of the data will be clearly set out before people opt-in. Clear provision will also be made for people to opt-out at any future date.

Automated Decision Making

The Abbey Line CRP does not make use of any automated decision systems.

Privacy Notice

A privacy notice will be set out on the ALCRP website and on any printed materials where people can sign up to receive communications from ALCRP.

Cookies

The Abbey Line Community Rail Partnership (ALCRP) uses cookies on its website to improve user experience, understand how the site is used, and ensure it functions effectively.

What are cookies?

Cookies are small text files placed on a user's device (computer, tablet, or mobile) when visiting a website. They help the website recognise the device and store certain information about preferences or past actions.

Types of cookies we may use:

- Essential cookies: Necessary for the operation of the website (e.g. enabling navigation and access to secure areas).
- Performance/analytics cookies: Help us understand how visitors use the website, so we can improve content and functionality.
- Functionality cookies: Remember user preferences to enhance the browsing experience.

Consent and control:

Where required, users will be asked to provide consent before non-essential cookies are placed on their device. Users can withdraw or modify their consent at any time via the cookie settings on the website.

Most web browsers also allow users to control or delete cookies through their browser settings. However, restricting cookies may impact the functionality of the website.

Data collected via cookies:

Any personal data collected through cookies will be processed in accordance with this Data Protection and GDPR Policy. Data will be:

- Used only for the stated purpose
- Kept secure
- Not shared with third parties without consent unless required by law

Third-party cookies:

Where the website uses third-party services (e.g. analytics providers), these may set their own cookies. ALCRP will ensure that any such providers are compliant with relevant data protection legislation.

Regulatory position

The Abbey Line Community Rail Partnership will comply with the Privacy and Electronic Communications Regulations (PECR), alongside UK GDPR, in relation to the use of cookies and similar technologies.

Low-risk cookies and consent

ALCRP recognises that regulatory changes may permit certain low-risk cookies (such as those used for basic analytics or essential functionality) to be set without explicit user consent, where they pose minimal impact on user privacy. Where this applies, ALCRP will ensure:

- The cookies are strictly limited in scope and purpose
- Clear information is still provided to users
- Users retain the ability to opt out where appropriate

For all other cookies, particularly those used for analytics, tracking, or third-party services, prior user consent will continue to be obtained in line with PECR requirements.

Penalty framework under PECR

ALCRP is aware that enforcement powers and penalty levels under PECR have been strengthened to align more closely with UK GDPR. As such, the organisation takes compliance seriously and will ensure that:

- Appropriate consent mechanisms are in place
- Cookie usage is regularly reviewed
- Records of consent are maintained where required

Failure to comply with PECR requirements may result in regulatory enforcement action, and ALCRP is committed to minimising this risk through good governance and transparent practices.

Further information:

More detailed information about the cookies used, their purpose, and duration will be provided in the website's Cookie Notice.

Sharing of Information

Personal information will not be shared with any third party, including other individuals on the database, unless there is express permission to do so. This includes the sharing of e-mail addresses – all mail outs will use 'bcc' rather than 'to' or 'cc'.

Complaints Process

Complaints will be handled via the Data Protection Complaints Process (see Appendix)

RESPONSIBILITY

Day-to-day responsibility rests with the CRP Officer.

In addition, there is a named individual on the CRP Steering Group who is the data protection champion.

USEFUL REFERENCES

Further advice on data protection can be found at:

<https://communityrail.org.uk/member-resources/data-protection-guidance/>

[The UK's New Amendments to the UK GDPR Become Law and Get a Nod from the EU. What happens now? | The Global Privacy Watch](#)

DATE OF ADOPTION: MAY 2026

REVIEW DATE: MAY 2029

APPENDIX

Data Protection Complaints Process

1. Submitting a Complaint

Individuals have the right to raise concerns about how their personal data is collected, used, or managed. Complaints can be submitted through the following channels:

- Email: info@abbeylinecommunityrail.org
- Post: Abbey Line CRP Officer; Hertfordshire County Council, Farnham House, SG1 2ST.

Complainants should include sufficient detail to allow the issue to be understood, including relevant dates, correspondence, and the nature of the concern.

2. Acknowledgement

All data protection complaints will be formally acknowledged within 30 calendar days of receipt. The acknowledgement will:

- Confirm that the complaint has been received
- Provide a contact point for further communication
- Outline the next steps and expected timelines

3. Complaint Handling and Response Process

The organisation will handle complaints in a fair, consistent, and timely manner:

1. Initial Review
 - The complaint will be assessed and logged.
 - A Data Protection Officer (DPO) or designated lead will be assigned.
2. Investigation
 - Relevant systems, records, and staff will be reviewed.
 - Additional information may be requested from the complainant if required.
3. Outcome and Response
 - A formal written response will be provided, typically within one calendar month of acknowledgement (in line with GDPR response expectations).
 - Where investigations are complex, this timeframe may be extended by up to two additional months; the complainant will be informed of the reasons for any delay.
4. Remedial Action

Where appropriate, corrective action will be taken (e.g. rectification, restriction of processing, procedural improvements).

4. Escalation and Complaints to the ICO

If a complainant is not satisfied with the outcome or handling of their complaint, they have the right to escalate the matter to the Information Commissioner's Office (ICO).

- Website: <https://ico.org.uk>

- Complaints should normally be made to the ICO within three months of the organisation's final response

Updated Procedural Expectations

- In line with current ICO guidance:
- Individuals are encouraged to raise concerns with the organisation first to allow resolution.
- Organisations must demonstrate accountability, including maintaining records of complaints and outcomes.
- Responses should be transparent, clear, and timely, with evidence of investigation.
- Failure to respond appropriately within expected timeframes may be considered by the ICO when assessing compliance.

5. Record Keeping

All complaints and their outcomes will be documented to support compliance with GDPR accountability requirements and continuous improvement of data protection practices.