RIVERWAY CARE

Data Protection and Information Governance Policy

This policy sets Riverway Care's framework for using personal information lawfully, fairly, transparently and securely. It gives particular attention to children's information, safeguarding records and workforce data.

Document control	Details
Document reference	RW GOV 002
Version and issue date	Version 1.0 | 9 October 2026
Approval status	Approved for issue
Approved by	Riverway Care Directors
Next review date	9 October 2027
Applies to	Directors, employees, workers, volunteers, contractors and anyone handling information for Riverway Care

1 Purpose and scope

Riverway Care will process personal information to plan and provide care, safeguard young people, recruit and support staff, work with commissioners and professionals, meet legal duties and operate the organisation. This policy applies to information in any format, location or system and to everyone acting on Riverway's behalf.

The policy supports the UK General Data Protection Regulation, the Data Protection Act 2018 and relevant changes made by the Data Use and Access Act 2025. Detailed privacy notices, a retention schedule, information-sharing procedures and breach arrangements support this policy.

2 Data protection principles

1. Process information lawfully, fairly and transparently.
2. Collect information for specified, explicit and legitimate purposes and do not use it incompatibly.
3. Collect only information that is adequate, relevant and limited to what is needed.
4. Keep information accurate and correct it when necessary.

5. Keep identifiable information no longer than necessary.
6. Protect information with appropriate security against unauthorised access, loss, damage or disclosure.
7. Be able to demonstrate compliance through decisions, records, training and review.

3 Governance and responsibilities

Role	Responsibilities
Directors	Accountable for compliance, resources, risk oversight and approving this policy.
Data protection lead	Coordinates privacy notices, rights requests, breaches, records of processing, retention, training and regulator contact. The role will be formally designated before operations begin.
Managers	Ensure local practice follows this policy, control access, maintain accurate records and escalate incidents promptly.
All workers	Use information only for authorised work, follow secure processes, keep credentials private and report mistakes or concerns immediately.
Processors and contractors	Process information only under an appropriate written contract and Riverway's documented instructions.

4 Information Riverway may process

- Identity, contact, family, placement, education, health, disability and care information about young people.
- Safeguarding, risk, incident, missing-from-care, behaviour support, complaints and advocacy records.
- Information about parents, carers, relatives, social workers, health and education professionals and other members of a young person's network.
- Recruitment, right-to-work, DBS, references, payroll, rota, training, supervision, performance, absence and occupational-health information.
- Professional contact, supplier, visitor, enquiry, referral, website and correspondence information.
- Images, audio, access-control or monitoring information where its use is lawful, necessary and proportionate.

5 Lawful use and special category information

Before processing begins, Riverway will identify and record an appropriate lawful basis. Depending on the purpose, this may include contract, legal obligation, vital interests, legitimate interests or a task carried out in the public interest where the law supports that basis. Consent will not be used where a person has no genuine choice or another basis is more appropriate.

Health, ethnicity, religion, sexual orientation, biometric data and other special category information require both an Article 6 basis and an Article 9 condition. Relevant conditions may include employment and social-protection law, health or social care, safeguarding, substantial public interest, legal claims or explicit consent. Criminal-offence data, including DBS information, will only be processed with appropriate legal authority and safeguards.

6 Children's information

Children merit specific protection. Information must be explained in clear, age-appropriate language and used in a way that supports their rights, safety and care. Access should follow role and need, not convenience. Staff must avoid unnecessary labels, distinguish fact from professional opinion and record the child's views where relevant.

Safeguarding information may be shared without consent when necessary and lawful to protect a child or another person. The reason, proportionality and recipient should be recorded unless doing so would create additional risk.

7 Transparency and privacy information

Riverway will provide privacy information when it collects personal data and, where information is obtained elsewhere, within the required period unless a lawful exception applies. Notices will identify the organisation, purposes, lawful bases, categories, sharing, retention, rights and complaint routes in clear language. Young people will receive information suitable for their age and understanding.

8 Information sharing

- Share the minimum information necessary for a clear and legitimate purpose.
- Confirm the recipient's identity, authority and secure contact route.
- Consider urgency, safeguarding duties, confidentiality and the person's reasonable expectations.
- Use information-sharing agreements where regular or higher-risk sharing requires them.
- Record significant decisions, including reasons for sharing or declining to share.
- Do not promise absolute confidentiality when safety or law may require disclosure.

9 Security and access

- Use individual accounts, strong authentication and access based on role and need.
- Keep paper records in secure storage and transport them only when authorised.
- Use approved systems and secure transfer methods for sensitive records; ordinary email should not be used where a safer approved route is required.

- Lock screens, protect devices, apply updates and report lost devices or suspicious messages immediately.
- Do not use personal accounts, unapproved messaging services or personal storage for Riverway information.
- Review access when roles change and remove it promptly when engagement ends.

10 Accuracy retention and disposal

Records will be checked and updated where appropriate. Riverway will maintain a retention schedule based on legal, regulatory, safeguarding, contractual and limitation requirements. Information subject to a complaint, investigation, legal hold or safeguarding need must not be destroyed until authorised. Disposal must prevent reconstruction, and disposal by a contractor must be evidenced.

11 Individual rights

People may have rights to access, correct, erase, restrict or object to processing, and to receive portable information. They may also have rights concerning automated decision-making. These rights are not absolute. Requests must be recognised, logged, identity-checked proportionately and answered within the applicable legal period. A child's competence, best interests and the rights of others must be considered when responding to requests involving care records.

12 Personal data breaches

8. Contain the incident without destroying evidence.
9. Report it immediately to the manager and data protection lead, including near misses.
10. Record what happened, information and people affected, likely consequences and action taken.
11. Assess risk to people's rights and freedoms and consider safeguarding notifications.
12. Notify the ICO without undue delay and, where required, within 72 hours of awareness.
13. Tell affected people without undue delay where the law requires it and provide practical protective advice.
14. Review causes and implement proportionate improvements.

13 Higher risk processing and suppliers

A data protection impact assessment will be completed before processing likely to create high risk, including significant new technology, systematic monitoring, large-scale special category data or innovative uses of children's information. Suppliers processing personal data must be assessed and engaged under contracts containing required data protection terms. International transfers require a lawful transfer mechanism and risk assessment where applicable.

14 Training assurance and review

Workers will receive data protection and information-security learning at induction and appropriate refreshers. Riverway will maintain records of processing, decisions, breaches, rights requests, contracts, retention and training as proportionate evidence of accountability. This policy will be reviewed at least annually and after material legal, service, technology or risk changes.

15 Questions and concerns

Questions and data protection concerns should be sent to hello@riverwaycare.co.uk. Individuals may also complain to the Information Commissioner's Office at https://ico.org.uk or by calling 0303 123 1113. Raising a concern with Riverway first may allow it to resolve the issue promptly, but this is not a requirement before contacting the ICO.

References and guidance

This document was developed for Riverway Care using the following legislation and official guidance. The sources should be checked when the document is reviewed.

- UK GDPR and Data Protection Act guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- ICO accountability and governance guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/
- ICO data protection by design guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/
- Information sharing advice for safeguarding practitioners: https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice