



Richmond House

Social Care Services CIC

General Data Protection Regulation (GDPR)

Privacy and Cookie Policy

2026 - 2027



PRIVACY AND COOKIE POLICY

Richmond House Social Care Service's Privacy Promise:

We're committed to protecting the privacy of our staff, customers and service users and believe in being upfront about how we collect and process data.

That's why, alongside our **GDPR Privacy Policy**, we've created our **Privacy Promise**. This quick and simple guide explains how we manage, share and look after your information in simple terms, so you can make informed choices about the data you share.

Our Privacy Promise:

We promise to collect, process, store and share your data safely and securely:

- **You're always in control:** Your privacy will be respected at all times and we put you in control of your privacy with easy-to-use tools and clear choices.
- **We work transparently:** We will be transparent about the data we collect and how we use that data so that you can make fully informed choices and decisions.
- **We operate securely:** We promise to protect the data you share with us by using appropriate security measures and controls. We're also careful with whom we allow to process your data on our behalf.
- **For your benefit:** We promise that when we do process your data, we will use it to benefit you and to make your experience better and to improve our products and services.

Privacy Policy:

This Privacy Policy is effective from **1 September 2026** and reflects the significant data protection reforms introduced by the **Data (Use and Access) Act 2025 (DUAA)**, which came into force on 5 February 2026. Our privacy policy will help you understand what information "Richmond House" collects, how we use it and what choices you have.



1. WHO WE ARE

Who is "The Richmond House"?

"Richmond House Social Care Services", "Richmond House Clubs", "Richmond House Short Break", "Richmond House Outreach Active" and "Richmond House Volunteer" (referred to in this policy as "we", "us" or "our") are trading names of:

The Richmond House

96 Main Street

North Frodingham

Driffield

East Riding of Yorkshire

YO25 8LJ

Registered Community Interest Company Number: 11154305

Our Data Protection Team

"The Richmond House" has appointed Mr Jumaa Al Karaki as a Data Protection Officer. They can be contacted in the following ways should you have any questions, complaints or feedback about your privacy:

Email: RichmondHouse@rhscs.org.uk

Mail to:

Data Protection Officer

The Richmond House



96 Main Street | North Frodingham

Driffield | East Riding of Yorkshire

YO25 8LJ

2. WHAT PERSONAL DATA DO WE COLLECT AND HOW DO WE USE IT

What data do we need and why we need it:

This section tells you what personal data we may collect from you, why we need it when you use our services and what other personal data we may receive from other sources.

We collect the data you provide to us:

- When you book your child for a camp
- When you speak to us over the phone or via email
- When you use the contact forms on our website
- When you apply for a job on the Richmond House website
- When you apply on the Richmond House's Volunteer website
- When you apply for a job with us.

We collect data when you use our services:

- Payment and transaction data
- Profile and usage data, including data we gather from the devices you use to connect to those services, such as computers and mobile phones, using cookies (please see our separate cookies policy) and other internet tracking software.

We collect data from third parties we work with:

- Social networks
- Public information sources
- Agents working on our behalf



The data we collect about you

We may collect, use, store and transfer different kinds of personal data about you, which we have grouped together as follows:

- **Identity data** – name, title, date of birth, gender, nationality and school details of those buying or using our services. For military staff, we also ask for service number, rank and place of work.
- **Contact data** – location, postcode, email address or telephone numbers.
- **Transaction data** – details of the products and services you have purchased from us, including date and time of booking and spend in relation to that transaction. We also collect the name on your payment card, your card number, expiry date and CVV number.
- **Technical data** – internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.
- **Profile data** – purchases or orders made by you, your interests, preferences, feedback and survey responses, preferences about the use of the services (including whether you are interested in certain events that we offer)
- **Usage data** – information about how you use our website and services.
- **Marketing and communications data** – your preferences in receiving marketing from us and your communication preferences.
- **Employment information** – Previous employment history, experience, relevant qualifications, work eligibility and references.
- **Criminal conviction and offence information** – In order to work for us, you will be required to undertake an enhanced Disclosure and Barring Service (DBS) check.
- **Health and Medical Information** – We will collect any relevant medical or health information of children who attend our camps, including first aid preferences. We also collate medical information, where supplied, for staff applying for select roles and employees.



We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data may be derived from your personal data, but is not considered personal data in law, as this data does not directly or indirectly reveal your identity. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data, which will be used in accordance with this privacy notice.

We do not collect any special categories of personal data about you, outside of those stated above. This includes details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data.

3. HOW WE USE YOUR PERSONAL INFORMATION

We are only allowed to use personal information about you if we have a legal basis to do so, and we are required to tell you what that legal basis is. We have set out in the table below: the personal information which we collect from you, how we use it, and the legal ground on which we rely when we use the personal information.

In some circumstances, we can use your personal information if it is in our legitimate interest to do so. The **Data (Use and Access) Act 2025 (DUAA)** has introduced significant changes to the lawful basis framework under UK GDPR. A new "**recognised legitimate interest**" lawful basis under Article 6(1)(ea) UK GDPR has been introduced, providing a set of pre-approved processing purposes deemed to be in the public interest. This is distinct from the existing "legitimate interests" basis under Article 6(1)(f), which remains available.

Recognised legitimate interests now include processing for:

- Direct marketing
- Intra-group transmission of personal data for internal administrative purposes



Richmond House Social Care Services CIC

- Network and information system security
- Crime prevention, public security, safeguarding, and emergency response
- Responding to public body requests

Where we rely on a recognised legitimate interest, we do not need to carry out an additional balancing test. However, we must still assess whether the processing is necessary for the purpose pursued, and the right to object continues to apply.

What do we use your personal information for	What personal information do we collect	Our legal grounds for processing	Our legitimate interests (if applicable)
To register you as a new customer	- Identity - Contact - Health & medical information	Performance of a contract with you	
To process and deliver your booking/purchase	- Identity - Contact - Transaction	- Performance of a contract with you - Legitimate interests	
To manage our relationship with you, including notifying you about changes to our terms or privacy notices	- Identity - Contact - Transaction	- Performance of a contract with you - Necessary to comply with a legal obligation - Legitimate interests	To keep our records up to date
To enable you to partake in a prize draw, competition or to complete a survey	- Identity - Contact - Transaction	- Performance of a contract with you - Legitimate interests - Consent	
To administer and protect our business and our website	- Transaction - Technical - Usage	- Legitimate interests	Running our business, provision of administration and IT services, network security
To deliver relevant website content and	- Identity - Contact - Marketing and	- Legitimate interests	To study how customers use our



advertisements to you and measure or understand the effectiveness of the advertising we serve to you	communications - Usage - Profile		services, to develop them, to grow our business and to inform our marketing strategy
To use Data Analytics to improve our website, products / services, marketing, customer relationships and experiences	- Technical - Usage - Profile	- Legitimate interests	To define types of customers for our services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy
To carry out a DBS check prior to employment	- Identity - Contact - Criminal Convictions & Offence information	- Performance of a contract - Legal obligation	
To make suggestions and recommendations to you about the services that may be of interest to you	- Identity - Contact - Marketing and communications - Technical - Profile - Usage	- Legitimate interests	To develop our services and grow our business

4. PROCESSING YOUR DATA USING OUR LEGITIMATE INTERESTS

We have a number of lawful reasons that we can use (or 'process') your personal data. One of these lawful reasons is called 'legitimate interests'.

Broadly speaking, legitimate interests mean that we can process your personal information if:

- We have a genuine and legitimate reason, and we are not harming any of your rights and interests.



The following are some examples of when and why we would use this approach during our normal course of business:

- **To improve and enhance our services:** When we do process your data, we will use it to benefit you, to make your experience better and to improve our products and services.
- **Your best interest:** Processing your information to protect you against fraud when transacting on our website, and to ensure our websites and systems are secure.
- **Personalisation:** Where the processing enables us to enhance, modify, personalise or otherwise improve our services/communications for the benefit of our customers.
- **Analytics:** To process your personal data for the purposes of customer analysis, assessment, profiling and direct marketing, on a personalised or aggregated basis, to help us with our services and to provide you with the most relevant information, as long as this does not harm any of your rights and interests.
- **Research:** To determine the effectiveness of promotional campaigns and advertising, and to develop our products, services, systems and relationships with you.
- **Direct Marketing:** We may send postal and email marketing. We will also make sure our postal and email marketing is relevant to you and tailored to your interests. You also have the right to opt out of receiving this information at any time by contacting us or updating your preferences.

When we process your personal information for our legitimate interests, we will consider and balance any potential impact on you and your rights under data protection and any other relevant law. Our legitimate business interests do not automatically override your interests – we will not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

5. WHO WE SHARE YOUR PERSONAL INFORMATION WITH



In order to provide you with our services and meet our legal obligations, we only share your data with 3rd parties in the following circumstances:

- To fulfil your order.
- To complete or confirm your location or postal address.
- To verify your identity and perform DBS checks.
- To authorise debit/credit card payments and any other transactions authorised by the supporter or customer.
- To manage and maintain the accuracy of your records.
- To handle complaints and improve customer service.
- To administer marketing on behalf of Richmond House.
- To meet legal obligations, for example, for national security, taxation and criminal investigations; and
- If Richmond House is acquired by a third party, in which case personal data held by it, about its customers, will be one of the transferred assets.

We'll never make your personal data available to anyone outside Richmond House for them to use for their own marketing purposes without your prior consent.



6. THIRD-PARTY LINKS

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice or policy of every website you visit.

7. TRANSFERRING YOUR PERSONAL INFORMATION OUTSIDE THE UK

The DUAA has introduced a more liberal 'risk-based' approach to international transfers of personal data. The key change is a revised statutory test: organisations must assess whether the standard of data protection in the transferee country is **"not materially lower"** than the standard in the UK. This replaces the previous adequacy framework and may facilitate increased transfers of personal data outside the UK.

We transfer your data outside of the UK in very limited circumstances. We have ensured that those organisations that we share your data with look after it securely and have appropriate safeguards, as required by UK GDPR (as amended by the DUAA), in place. These organisations are:

- **"Clickatell"** (Clickatell Limited, Bank House, 81 St Judes Road, Englefield Green, Surrey, TW20 0DF, UK) – Who provide a customer communication and messaging tool. – Clickatell may transfer your data to the US or South Africa whilst complying with applicable local data protection measures.
- **"Facebook"** (Facebook Inc, 1 Hacker Way, Menlo Park, CA 94025, USA) – Facebook provide a social media platform. – Facebook provides appropriate safeguards including the EU-US Data Privacy Framework and an appointed EU representative.
- **"Google"** (Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) – Google provide an analytics service – Google provides appropriate safeguards including the EU-US Data Privacy Framework.



- **"LinkedIn"** (LinkedIn Corporation, 1000 W. Maude Avenue, Sunnyvale, CA 94085, USA) – LinkedIn provide a social media platform. – LinkedIn provides appropriate safeguards including the EU-US Data Privacy Framework.
 - **"MailChimp"** (The Rocket Science Group LLC, 675 Ponce de Leon Avenue NE, Suite 5000, Atlanta, GA 30308, USA) – Provide our email communication platform – MailChimp provides appropriate safeguards including the EU-US Data Privacy Framework.
 - **"Snap Engage"** (Snap Engage LLC, 1722 14th St., Suite 220, Boulder, CO 80302, USA) – Provide our live chat feature – Snap Engage provides appropriate safeguards.
 - **"Survey Monkey"** (SurveyMonkey Inc., 1 Curiosity Way, San Mateo, CA 94403, USA) – Provide our survey platform – Survey Monkey provides appropriate safeguards including the EU-US Data Privacy Framework.
-

8. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator (including the ICO) of a breach where we are legally required to do so.



9. HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?

We will keep your personal information for as long as you are our customer or employee.

[Customer]

After you stop being an active customer, because you have stopped regularly using our services or buying our products, we may keep your personal information for up to 7 years for one of the following reasons:

- To respond to any questions or complaints from you;
- To maintain our records;
- To comply with laws applicable to us.

After such time, we will securely delete your personal information. If we receive a bounce back from any of the emails that we send to you on a number of occasions, we will delete your personal information in relation to those emails.

[Employee]

For permanent employees, we keep personnel files for 7 years after an employment contract has ended. This information includes, but is not exclusive to, employment contracts, training records and salary information. For temporary staff, we keep relevant records for 2 years.

This excludes members of the Senior Leadership Team, whose details are retained permanently.

10. MARKETING

We may use your personal information to tell you about relevant services and any upcoming offers. We can only use your personal information to send you marketing messages if we have either your consent or a legitimate interest to do so. Under the DUAA, **direct marketing** is now recognised as a legitimate interest under Article 6(1)(f) UK GDPR. Where we rely on this basis, we must still respect your right to object.



You can ask us to stop sending you marketing messages at any time – you just need to contact us or use the opt-out links on any marketing message sent to you. If you have set up an online account with us, then you can also change your communication preferences at any time.

Where you opt out of receiving marketing messages, this will not apply to personal data provided to us as a result of purchasing our services or any other transaction between you and us.

11. COOKIES AND TRACKING TECHNOLOGIES

The DUAA has introduced significant changes to the ePrivacy regime governing the use of cookies and other tracking technologies:

- **Increased fines:** Unlawful use of tracking technologies (e.g., cookies) is now subject to increased fines equivalent to those under the UK GDPR – up to the greater of **£17,500,000 or 4% of an undertaking's total annual worldwide turnover**, compared with a previous maximum of £500,000.
- **Personal liability:** Officers (e.g., directors) may now be subject to personal penalties of up to £17,500,000 for certain infringements of the ePrivacy regime.
- **Cookie exemptions:** Certain analytics and functionality cookies are now exempt from the PECR consent requirement.

The ICO published its final guidance on storage and access technologies on 29 April 2026, setting out how organisations can comply with PECR and, where relevant, the UK GDPR. This guidance covers cookies, tracking pixels, device fingerprinting, and scripts or tags. The PECR remain clear that, subject to limited exceptions, organisations must not deploy storage and access technologies unless they:

1. Tell subscribers or users what the technologies are;
2. Explain what they do; and
3. Obtain prior consent for their use



Exceptions include where the technology is:

- **Strictly necessary** to provide the service requested (e.g., security, fraud prevention, authentication)
- Used **solely for statistical purposes** about the use of the service

For full details, please see our separate Cookies Policy.

12. YOUR RIGHTS

Right to be Informed

We will always be transparent in the way we use your personal data. You will be fully informed about the processing through relevant privacy notices.

Right to Access

You have a right to request access to the personal data that we hold about you. Under the DUAA, a new **Article 12A UK GDPR** has been introduced which changes how the one-month subject access request (DSAR) period is calculated. The period is now measured from the **"relevant time"**, which is the latest of:

- Receipt of the request
- Receipt of any identity confirmation requested under Article 12(6)
- Payment of any fee

A new **"stop-the-clock"** provision applies: where we ask you for further information to identify the scope of your request, the period from that request to receipt of the information does not count towards the applicable time period. This applies where we reasonably require the information – for example, where we hold a high volume of data about you.

If you would like to request a copy of your personal data, please contact us in writing.

Right to Rectification



We want to make sure that the personal data we hold about you is accurate and up to date. If any of your details are incorrect, please let us know and we will amend them.

Right to Erasure

You have the right to have your data 'erased' in the following situations:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed.
- When you withdraw consent.
- When you object to the processing, and there is no overriding legitimate interest in continuing the processing.
- When the personal data was unlawfully processed.
- When the personal data has to be erased in order to comply with a legal obligation.

If you would like to request the erasure of your personal data, please contact us in writing. Please note that each request will be reviewed on a case-by-case basis, and where we have a lawful reason to retain the data, it may not be erased.

Right to Restrict Processing

You have the right to restrict processing in certain situations, such as:

- Where you contest the accuracy of your personal data, we will restrict the processing until you have verified the accuracy of your personal data.
- Where you have objected to processing, and we are considering whether Richmond House's legitimate grounds override your legitimate grounds.
- When processing is unlawful, you oppose erasure and request restriction instead.
- Where Richmond House no longer need the personal data, but you require the data to establish, exercise or defend a legal claim.

Right to Data Portability

You have the right to data portability in certain situations. You have the right to obtain and reuse your personal data for your own purposes via a machine-readable format, such as a



CSV file. If you would like to request portability of your personal data, please contact us by writing to us. This only applies:

- To the personal data that you have provided to us;
- Where the processing is based on your consent or for the performance of a contract; and
- When processing is carried out by automated means.

Right to Object

You have the right to object to Richmond House processing your data in these circumstances:

- Where the processing is for direct marketing. Remember, you can opt out of email communication at any time via the unsubscribe feature on our emails.
- Where the processing is based on legitimate interests (including recognised legitimate interests under the DUAA);
- Where the processing is for purposes of scientific/historical research and statistics.

Right to Lodge a Complaint

From **19 June 2026**, all controllers (including Richmond House) must operate a formal complaints procedure for data subjects. This includes:

- A requirement to acknowledge data protection complaints **within 30 days**
- A requirement to respond **without undue delay**

13. AUTOMATED DECISION-MAKING

The DUAA has significantly reformed the framework for automated decision-making (ADM). **Article 22 of the UK GDPR** (which previously prohibited solely automated decision-making) has been replaced with **new Articles 22A to 22D**, moving from a prohibition to a **permission-plus-safeguards model**.



This reform aims to promote innovation and the use of AI systems. The requirement to establish a qualifying lawful basis before conducting ADM (previously at Article 22(2) UK GDPR) has been removed, except where special category data is used. Data subjects will still benefit from rights of objection and human intervention.

Richmond House does not currently use solely automated decision-making that produces legal or similarly significant effects concerning you. If this changes, we will update this policy and notify you accordingly.

14. CHILDREN'S PERSONAL DATA

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. The ICO has published guidance on the processing of children's personal data, and we comply with this guidance in all our processing activities involving children.

15. THE REGULATOR

- If you feel that The Richmond House has not upheld your rights, we ask that you contact our Data Protection Officer, whose details can be found in point 1, so that we can try and help.
- If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you have the right to lodge a complaint with the Information Commissioner's Office (ICO). Their details are supplied below:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow



Richmond House Social Care Services CIC

Cheshire

SK9 5AF

Telephone: 0303 123 1113

Website: www.ico.org.uk

16. HOW TO CONTACT US

Address:

The Richmond House

96 Main Street

North Frodingham

Driffield

East Riding of Yorkshire

YO25 8LJ

Tel. 07484371525

Reviewed by: Hala Okasheh **Date:** 01/09/2026

Authorised by: Jay Al Karaki **Date:** 01/09/2026

Document Version: Vr 08

Review Period: 2026 – 2027



Next Review: 1 September 2027 or sooner if statutory guidance changes.

Summary of Key Legislative Updates (2026–2027)

Update	Key Changes
Data (Use and Access) Act 2025 (DUAA) Commencement	Principal data protection provisions came into force on 5 February 2026
New Lawful Basis – Recognised Legitimate Interest	Article 6(1)(ea) UK GDPR introduced; five categories of recognised legitimate interest requiring no balancing test
Subject Access Requests (DSARs)	New Article 12A UK GDPR changes how the one-month period is calculated; "stop-the-clock" provision introduced
Automated Decision-Making	Articles 22A–22D replace Article 22; moves from prohibition to safeguards regime
International Transfers	New "not materially lower" test replaces previous adequacy framework
PECR Fines	Increased to UK GDPR levels – up to £17.5 million or 4% of global turnover
Cookie Exemptions	Certain analytics and functionality cookies exempt from PECR consent requirement
Complaints Procedure	New section 164A DPA 2018 requires controllers to acknowledge complaints within 30 days; in force from 19 June 2026
ICO Guidance	Final guidance on recognised legitimate interest (23 March 2026), storage and access technologies (29 April 2026), purpose limitation (23 March 2026), and international transfers (15 January 2026)

This Privacy and Cookie Policy should be read in conjunction with Richmond House's other policies and procedures, including our Data Protection Policy and Safeguarding Policy.