Privacy Policy (incorporating Cookie Policy)

This Policy applies to Ciphr Benefits Group Limited (registered in England and Wales - company no. 05421032) and its subsidiary companies, Ciphr Benefits Limited and Ciphr Benefits Systems Limited.

We are strongly committed to protecting personal data. This Policy describes why and how we collect and use personal data and provides information about individuals' rights. It applies to personal data provided to us, both by individuals themselves or by others. We may use personal data provided to us for any of the purposes described in this privacy statement or as otherwise stated at the point of collection.

We operate the following software platforms, which are licensed by us to our customers:

Perkpal.co.uk, Benefit-Select.co.uk, FlexGenius.co.uk, WorkplaceOne.co.uk

GDPR Principles

The following principles are complied with when processing personal data:

- Data is processed fairly and lawfully
- Data is processed only for specified and lawful purposes
- Processed data is adequate, relevant and not excessive
- Processed data is accurate and, where necessary, kept up to date
- Data is not kept longer than necessary
- Data is processed in accordance with an individual's consent and rights
- Data is kept secure
- Data is not transferred to countries outside of the European Economic Area (EEA) without adequate protection

Data Controller and Data Processor

In the majority of cases, we act as a Data Processor. As a Data Processor, we act under an agreement with, and on the written instructions of a Data Controller. The Data Controller is usually the employer of the individual (Data Subject) and will have a Privacy Policy in place that determines the following:

1. Lawful Basis of Processing Data

The lawful basis of processing of data will always be determined prior to any data being processed. The options for processing personal data under the GDPR are as follows:

- Consent – the individual has given their Consent to the processing of their personal data
- Contractual – processing of personal data is necessary for the performance of a contract to which the individual is a party, or for us to take pre-contractual steps at the request of the individual
- Legal Obligation – processing of personal data is necessary for compliance with a legal obligation to which we are subject
- Legitimate Interests – processing of personal data is necessary under our Legitimate Interests or those of a Third Party, unless those interests are overridden by the individual's interest or fundamental rights

- Public Task – processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- Vital Interests – processing of personal data is necessary to protect the vital interests of the individual or another individual

2. Type of Personal Data Being Processed

The type of personal data being processed will depend on the services available under each software platform and may include but is not limited to:

- Name
- Address
- Email Address
- Job Title
- Telephone Number
- IP Address
- Home Address
- Dependant details
- Date of Birth
- Remuneration

3. How Personal Data is Collected

Personal data is obtained from one or more of the following:

- Visits and use of our websites
- Parties entering into agreements with us
- Employment enquiries

4. Why Personal Data is Collected

Personal data is collected to provide legitimate business services which include:

- For us to review and reply to your enquiry
- To meet our statutory monitoring and reporting responsibilities
- To handle and communicate offerings, administration of offerings, delivery of products and services

Where indicated, however, some of the information is optional and you can choose not to complete.

5. How Personal Data is Used

Personal data may be used to:

- Process orders, process a request for further information, to maintain records and to provide pre and after-sales service
- Pass to another organisation to supply/deliver products or services you have purchased and/or to provide pre or after-sales service
- Carry out our obligations arising from any contracts entered into by you and us
- Comply with legal requirements
- We may need to pass the information we collect to other companies within our Group for administrative purposes
- Seek your views or comments on the services we provide
- Notify you of changes to our services

- Send you communications which you have requested and that may be of interest to you. These may include information about product updates, newsletters, events, webinars
- To inform you of various promotions, goods and services that may be of interest to you. You may be contacted by post, email, telephone, SMS or such other means with carefully selected marketing communications we deem relevant to send to you in the course of pursuing our legitimate interests.
- Create a profile of your interests and preferences so that we can contact you with information relevant to you. We may make use of additional information about you when it is available from external sources to help us do this effectively

6. Where Personal Data is Stored

Information collected is stored on our websites. As part of any services we offer, information provided will not be transferred to or located in a country outside the UK or EEA.

7. For how long is Personal Data Stored

We review our retention periods for personal data on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations. We will hold personal data on our systems for as long as is necessary for the relevant activity, or as long as is set out in any relevant contract you hold with us.

8. Who has Access to Personal Data

Only employees of ours with absolute need are granted access to customer information. This is ensured by the use of strict operational processes and procedures.

Technical and Organisation Measure to Protect your Data

Our Staff are trained on security systems and relevant processes and procedures which are reviewed regularly for ongoing effectiveness and suitability for purpose. All employees are kept up-to-date with our security and privacy practices. Employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure that customer information is protected.

Personal information provided via the Company's portals is encrypted in transit using Transport Layer Security (TLS). All traffic to and from the platform runs over HTTPS, and non-secure connections are automatically redirected to the secure (HTTPS) equivalent. Modern web browsers indicate a secure connection with a padlock icon in the address bar. Information supplied on these pages is securely stored and can only be accessed for the purposes for which it was provided.

All IT systems are kept in a secure environment with appropriate access control.

Non-sensitive details (your email address and other requested information) are transmitted normally over the Internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

We will not sell or rent your information to third parties.

Third-Party Service Providers working on our behalf:

We may pass your information to our third-party service providers, agents, subcontractors and other associated organisations for the purposes of completing tasks and providing services to you on our behalf. However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service and we have a contract in place that requires them to keep your information secure.

Third-Party Product Providers we work in association with:

We work closely with various third-party product providers to bring you a range of quality and reliable products and services designed to meet your needs. When you enquire about or purchase one or more of these products, the relevant third-party product provider will use your details to provide you with information and carry out their obligations arising from any contracts you have entered into with them. In some cases, they will be acting as a data controller of your information and, therefore, we advise you to read their Privacy Policy. These third-party product providers will share your information with us which we will use in accordance with this Privacy Policy.

We may transfer your personal information to a third party as part of a sale of some or all of our business and assets to any third party including for a merger, acquisition, divestiture, or similar transaction or as part of any business restructuring or reorganisation.

We may also further transfer data if we are under a duty to disclose or share your personal data in order to comply with any legal obligation or to law enforcement. However, we will take steps with the aim of ensuring that your privacy rights continue to be protected.

Individuals' Rights

Different rules apply depending on the type of Lawful Processing being undertaken. Many of the following individuals' rights apply, however, whatever the basis of processing:

- The right to be informed how personal data is processed
- The right of access to their personal data
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

The accuracy of personal data is imperative. We aim to keep it updated at all times.

The personal data we hold on you is available upon request by contacting the Data Controller, which in most cases will be your employer. You can request that your data is updated and/or deleted at any time, unless the Data Controller can justify that it is retained for legitimate business or legal purpose. When updating your personal data, you may be asked to verify your identity before your request can be actioned.

Links to other websites/from other websites

Our websites may contain links to other websites run by other organisations. Our Privacy Policy only applies to our websites and you are encouraged to read the Privacy Statements on the third party websites that you visit. We are not responsible for the Privacy Policies and practices of other websites even if they were accessed via one of our websites. Equally, if you link to one of our websites from a third-party site, we are not responsible for the Privacy Policies and practices of that third-party site.

Questions and Subject Access Requests (SARs)

Any questions or Subject Access Requests (SARs) should be directed to the Data Controller which in most cases will be your employer.

You have a right to lodge a complaint in the event that you believe that we have not upheld the rights, obligations and responsibilities as set out in this Policy. Please send any complaint to: dpo@ciphr.com

Cookie Policy

We use a number of cookies on our websites to enable us to provide visitors with the best user experience possible while navigating our sites; by using our site visitors implicitly agree to our use of cookies.

We take the privacy of our customers and the visitors to our site very seriously; if you want to know more about cookie management, we provide an explanation and links to more information on how you can manage cookies in your browser below.

We provide specific details about the cookies we use and the reasons for using these cookies to enable site visitors to make an informed decision and thus provide informed consent. Our primary reason for using cookies is to enable key site functionality, without which users would be unable to access essential features of our system.

What are Cookies?

The use of Cookies and similar technologies has for some time been commonplace and cookies in particular are important in the provision of many online services.

Cookie scope – Session VS Persistent Cookies

Cookies can expire at the end of a browser session (from when a user opens the browser window to when they exit the browser) or they can be stored for longer.

- **Session cookies** – Allow websites to link the actions of a user during a browser session. They may be used for a variety of purposes such as remembering what a user has put in their shopping basket as they browse around a site. They could also be used for security when a user is accessing internet banking or to facilitate use of webmail. These session cookies expire after a browser session so would not be stored long term. For this reason, session cookies may sometimes be considered less privacy intrusive than persistent cookies.

- **Persistent cookies** – Are stored on a user's device in between browser sessions which allows the preferences or actions of the user across a site (or in some cases across different websites) to be remembered. Persistent cookies may be used for a variety of purposes including remembering users' preferences and choices when using a site or to target advertising.

Cookie Sources – First VS Third party

Whether a cookie is 'first' or 'third' party refers to the website or domain placing the cookie.

First party cookies in basic terms are cookies set by a website visited by the user - the website displayed in the URL window.

Third party cookies are cookies that are set by a domain other than the one being visited by the user. If a user visits a website and a separate company sets a cookie through that website this would be a third party cookie.

Managing Cookies

You can control what cookies can be set on your computer. For more information on specific requirements please refer to your web browser help file or for more information please check here.

What Cookies are used on our sites and why we use them?

The following list provides a comprehensive overview of the Cookies used on our site and what tool or technology each is used for and why we are using each tool.

This list includes cookies deployed by third parties on our websites. By using this website you are agreeing to our T&Cs, Privacy and cookie policies and consent to the use of cookies and similar technologies by us and our carefully selected third party partners as described in these policies.

If you do not agree to such use, please see the Managing Cookies section for details on how to adjust your settings.

We will update this list as we make changes to the shopping experience on our websites, mobile website and mobile applications.

Cookie ID(s)	Associated Solution/Technology	Why we are using the Cookie
AcceptedCookies	MyWorkPal	Used to track a user has accepted the cookie policy warning
Torus	MyWorkPal	Used to authenticate a user on the website
returnPath	MyWorkPal	Used to track a user's navigation through the site in order to place them

		back at the right point when they log back in after session expiry
_ga _gat _gid __utma __utmc __utmz	Google Analytics – Universal	We use Google Analytics to help us understand how visitors navigate to and through our website. These cookies enable the function of Google analytics. This service helps us evaluate how long customers spend visiting different pages and how often they return to our website. You can find out how to opt out of these cookies here and More Information about google analytics here.
AcceptedVersionUpdate	MyWorkPal Admin	Used to track a user has accepted the version update warning on the admin portal

ARRAffinity	Microsoft Azure Cookie. Ensures requests from your browser are consistently routed to the same server during your session, maintaining performance and stability. Strictly necessary for the website to function and cannot be disabled.
ARRAffinitySameSite	Microsoft Azure Cookie. Same purpose as ARRAffinity; set with SameSite=None to support cross-site request routing in modern browsers. Strictly necessary for the website to function and cannot be disabled.
PrivacyPolicy	Set when a user accepts the privacy policy notice. Stores a flag so the acceptance banner is not shown again on repeat visits. It does not track activity or store any personal information. Duration 6 months.

We regularly review our use of cookies and we update this page regularly. However, there may occasionally be instances when cookies used are missing from the list. If you identify any that are not on the list please email us at dpo@ciphr.com with as much information as possible and we will do our best to quickly investigate this for you and then update our list as required.

Complaints

You have a right to lodge a complaint in the event that you believe that we have not upheld the rights, obligations and responsibilities as set out in this Policy. Please send any complaints to: dpo@ciphr.com.

Review of this Policy

This Policy is regularly reviewed. It was last updated 31st July 2026.