Privacy Notice

This privacy notice is effective as of January 2026 and will be updated regularly to reflect any changes in how we handle your personal data or in applicable laws.

Introduction

Xperience takes your right to privacy and the protection of your data seriously. Our aim is to make you feel secure when you deal with us - your personal data is in safe hands.

We will handle your personal data in compliance with relevant laws and our internal data privacy policies. We have organisational and technical measures in place to protect your personal data against unauthorised or unlawful processing, accidental loss, alteration, disclosure, access, destruction, or damage.

This page contains information about how Xperience Group (“Xperience”, “we”, "us" or "our") collect and use personal data about you (“your personal data”; “your data”). It also outlines your rights in relation to the processing of your personal data.

There is a separate Privacy Notice that explains how we handle employee’s personal data.

Categories of Personal Data We Collect and Use

Xperience gathers personal data from potential employees, clients, suppliers, business contacts, shareholders, and website users.

If you provide personal data about someone else (such as a referral), you are responsible for ensuring the individual is informed of the details contained in this privacy notice.

We collect data directly from you (for example, when you sign up for a newsletter or register to download website content) and indirectly from certain third parties, including our public websites, social media, suppliers, and vendors.

Sensitive Data Handling

Xperience does not intentionally or knowingly collect or process special category data or criminal offence data when acting as a Controller for clients, suppliers or website users. This means that data relating to characteristics such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health information, biometric or genetic data, sexual orientation, or criminal convictions and offences is not sought or processed in these contexts.

Pre-Employment Screening and Criminal Record Checks

Our pre-employment screening process involves the collection of certain sensitive data and is managed either by our People Team or, in specific circumstances, by an external provider. This process is essential to ensure compliance with relevant legislation and to support our commitment to a fair and safe working environment.

Candidates are required to complete a pre-employment health questionnaire, legally mandated under the Equality Act 2010 and the Disability Discrimination Act 1995. This is to identify whether additional support may be necessary for disabled employees, thereby ensuring that no individual is subject to unlawful or less favourable treatment throughout the recruitment and selection process.

Additionally, our process includes obtaining a criminal records check from the Disclosure and Barring Service. This check may be conducted for individuals applying for employment, current employees, contractors, agency workers, and members of the Board. These checks are particularly required for roles involving regulated activities, as outlined in the Safeguarding of Vulnerable Groups Act 2006. Such activities typically include positions that involve working with children or vulnerable adults, especially in establishments such as schools.

Individuals who are required to undergo these checks will be notified during the recruitment process. All practices relating to pre-employment screening and criminal records checks are governed by our Recruitment and Selection Policy and Criminal Record Check Policy, both of which are available on our Careers website. Should you need further information or clarification, please do not hesitate to contact us.

Personal Data Collection on Our Website

When you access our website, certain technical information is automatically collected, such as your computer's IP address, operating system, and browser type. This includes information entered on forms, newsletter subscriptions, event registrations, and data captured through website technologies. From time to time, we may invite you to participate in surveys designed to enhance the user experience on our website. If you choose to provide your details, we may keep a record of our correspondence with you. The provision of such personal data is entirely voluntary.

This data is used for purposes including system administration, filtering site traffic, performing domain lookups, and preparing statistical reports. Alongside these technical details, we record information about your activity on our website, such as the specific pages you visit, resources you view or download, and any associated communication data.

Use of Cookies

We employ cookies and similar technologies, including pixel tags and tracking links, to gather information during your interactions with our website. These tools are essential for improving both our products and services, and for enhancing the website's functionality and performance. Additionally, cookies help streamline your experience by remembering your details, which saves you time when revisiting the site.

In some cases, we may collect information regarding your activity on other websites. This enables us to deliver advertising content tailored to your interests and to further develop our offerings.

For more information about these technologies and guidance on how to manage your privacy settings through your browser, please refer to our Cookie Notice.

Links to Third-Party Websites and Programmes

Our websites may contain links to partner network sites and selected third-party programmes. Please note that these third parties may process your personal data for their own purposes. Xperience does not accept responsibility or liability for the privacy practices of third-party sites or programmes.

Personal Data Collection at Our Offices

When you visit our offices, we will request your details for visitor sign-in and, in some cases, provide a temporary access pass.

We operate closed-circuit television (CCTV) systems on our premises for the following purposes:

- Ensuring the safety and security of staff, visitors, and property.
- Preventing and detecting crime or misconduct.
- Supporting health and safety compliance.
- Monitoring access to restricted areas.

This is part of our ISO 27001 certification and ensures we maintain the security of our data by knowing who is present on our premises.

Use of Personal Data for Marketing

Sources of Marketing Data

We source marketing data from individuals who subscribe to newsletters, download marketing collateral, attend events, engage in sales discussions, or conduct business with us. We may also obtain contact information from publicly available sources, such as social media websites and data providers, such as ZoomInfo to make initial contact with relevant individuals at clients or other companies.

ZoomInfo collects business contact information related to individuals and uses this information to create professional profiles of individuals and profiles of businesses. This is used by us for business-to-business sales and marketing activities. ZoomInfo Privacy Centre can be found at zoominfo.com/trust-center.

Targeted Emails

We send targeted commercial emails to individuals and companies with whom we have business relationships or who have expressed interest in our products and services and opted in to receive emails. Our targeted emails track whether messages are opened, read, deleted, or whether links are clicked. Clicking a link will direct you to our website, where you will be prompted to accept our cookie policy.

Communications will always include the option to unsubscribe at any time from future communications.

Customer Relationship Management (CRM)

We maintain a CRM system to track and manage sales and marketing activities. The database contains personal data for individuals at client companies, suppliers, and other organisations with whom we have or wish to develop business relationships. Information includes contact details, purchased products or solutions, potential interests, and publicly available data from social media, as well as engagement with commercial emails or website activity.

Purposes and Legal Bases for Processing Personal Data

Xperience processes your personal data solely for specific purposes. The following table lists these purposes and the corresponding legal basis for each:

Purpose	Legal Basis
Recruitment – advertising, application, and onboarding stages, including pre-employment checks.	Legitimate Interest – facilitating recruitment of suitable employees before a contract is formed.

	Employment and social security law obligations – e.g. health data for sick leave, diversity monitoring, or reasonable adjustments (Equality Act 2010). Protecting the public / regulatory requirement – criminal offence checks to prevent people from completing work for which they are unsuitable.
Communicating with existing customers - such as service updates, maintenance notifications, delivery information and account-related alerts.	Contractual necessity – required to deliver a service and maintain necessary communication.
Delivery of our core services.	Contractual necessity – required to deliver contracted services (e.g. IT support, business applications, cyber security).
Operating and managing our business.	Legitimate Interest – ensuring efficient business operations.
Legal compliance.	Legal obligation – necessary to comply with the law.
Monitoring your use of our systems.	Legitimate Interest – compliance and protection of our reputation.
Social listening.	Legitimate Interest – protecting our assets and brand on social media using publicly accessible content only.
Reviewing website, network, and information security.	Legitimate Interest – ensuring optimal user experience and IT security.
Data analysis to improve company performance.	Legitimate Interest – supporting effective business operations.
Marketing to prospective customers via email or telephone.	Legitimate Interest – providing business value and developing new services; communications include an unsubscribe option.
Marketing to existing customers via email or telephone.	Legitimate Interest – informing customers about complementary services; supports ongoing development of offerings.
Use of cookies or similar technology.	Consent – by using our website, you consent to cookies as outlined in our Cookie Policy.
Access control and CCTV in our offices.	Legitimate interest - maintaining a safe and secure environment.

We process your personal data only for the purposes listed above. We will not use your data for any other purposes unless required or authorised by law, or in your vital interests, such as during a medical emergency.

Sharing Your Personal Data with other organisations

We may disclose the personal data We hold about you to any company within the Xperience Group when this is necessary to deliver our services.

We only share personal data with third parties when necessary for contractual agreements with clients, or when working with trusted partners to provide services. We have Data Processing Agreements in place with our Data Processors. This means that they cannot do anything with your personal data unless we have instructed them to do it. They will not share your personal data with any organisation apart from us or further Sub-Processors who must comply with a Data Processing Agreement. They will hold your personal data securely and retain it for the period we instruct. Further, they must process the personal data in accordance with this Privacy Notice and as permitted by applicable data protection laws. For instance, personal data may be shared for software licencing and warranty registration with

third-party vendors or for third-level support with companies such as Microsoft, Sage, Infor, IBM, or Sophos.

We may, from time to time, expand or reduce our business and this may involve the sale and/or the transfer of control of all or part of our business. Any personal data that you have provided will, where it is relevant be transferred and the new owner or newly controlling party will, under the terms of this Privacy Notice, be permitted to use that data only for the purposes for which it was originally collected by us.

International Data Transfers

Your personal data may be transferred outside the United Kingdom. Xperience ensures that appropriate safeguards are in place, including Adequacy Decisions and International Data Transfer Agreements, to protect your data in accordance with data protection laws.

Xperience transfers limited personal data to South Africa to provide helpdesk and project support, business analysis and as part of our recruitment process. Only the necessary information is processed, and robust security measures are in place. When you interact with our service desk, project teams or apply for a job with us, your information may be transferred to operatives in South Africa.

Job candidates

As part of our recruitment process, some stages of candidate data processing may be carried out by authorised personnel based in South Africa. This includes activities such as application review, candidate communication, and interview coordination.

We ensure that:

- Candidate personal data transferred to South Africa is protected using approved international transfer mechanisms, including the UK's International Data Transfer Agreement (IDTA) or Standard Contractual Clauses (SCCs).
- Appropriate technical and organisational measures (such as encryption, access controls, and monitored systems) are in place to safeguard your data.
- The individuals processing your data are bound by confidentiality obligations and receive appropriate data protection training.
- No data is transferred onward from South Africa to any other country without our authorisation.

Your data protection rights under the UK GDPR remain fully intact, irrespective of where processing occurs.

Data Security

We maintain rigorous organisational, physical and technical security arrangements to protect your personal data. These arrangements are supported by protocols, policies, procedures, and guidance designed to minimise risks. Our security measures include:

- ISO27001 certification, confirming our effective Information Security Management System.
- Regular penetration testing to maintain robust technical defences.
- Regular training for employees.
- Access to your personal information is strictly on a 'need to know' basis.

- Procedures to deal with any actual or suspected personal information breach, including notification to regulators when required.

Data Retention

We only keep personal data for as long as is reasonably required for the purposes explained in this Privacy Notice. We do keep certain transactional records - which may include personal data - for more extended periods to meet legal, regulatory, tax or accounting needs. For instance, we are required to retain an accurate record of dealings with us, so we can respond to any complaints or challenges you or others might raise later. We will also retain files if we reasonably believe there is a prospect of litigation.

To support us in managing how long we hold your data and our record management, we maintain a Record Retention Policy which includes clear guidelines on data retention and deletion.

We may also retain personal data in an aggregated form which allows us to continue to develop/improve our products and services.

Your Rights Regarding Your Personal Data

You are entitled, subject to certain conditions and exceptions under applicable laws, to exercise the following rights:

- Access Your Personal Data: Confirm that your data is being processed and verify its lawfulness.
- Correct Mistakes: Instruct us to rectify any inaccuracies.
- Right to be Forgotten: Request erasure of your personal data.
- Stop Processing: Request cessation of processing your personal data.
- Data Portability: Request transfer of your data to another organisation in certain circumstances.
- Object to Direct Marketing: Object to your data being processed for marketing purposes.
- Object to Profiling: Under specific circumstances, object to profiling or automated decision-making.
- Right to Complain: Lodge complaints with the Information Commissioners Office (ICO) at ico.org.uk. Before doing so, please contact compliance@xperience-group.com to exercise your rights or ask questions about data processing.

If you believe your data privacy rights have not been respected, we encourage you to seek resolution with Xperience first. Please email your request to compliance@xperience-group.com.

Contact Us

If you have any questions, please contact us at:

- Email: compliance@xperience-group.com
- Write to: Data Protection Representative, Xperience, Knockmore Hill Industrial Park, 11 Ferguson Drive, Lisburn, Co. Antrim, BT28 2EX, Northern Ireland