

OMERS Employee Privacy Statement

PRIVACY



Karen Tsang



Effective
March 1, 2026

OUR COMMITMENT TO YOUR PRIVACY

At OMERS, honesty and integrity are at the core of everything we do. We are committed to building and keeping your trust in all aspects of our operations, including how we handle your personal data. Throughout our operations we implement privacy practices designed to help keep your personal data safe, secure and used appropriately. We hope this Privacy Statement will help you to understand our approach to employee privacy.

This Privacy Statement applies to the collection, use, storage, and disclosure of personal data of our current, prospective and former employees and Designated Contractors across OMERS, which for clarity, includes Oxford.

What type of personal data do we collect?

In the course of operations, OMERS collects personal data about you. Examples of personal data that OMERS may collect includes:

- basic contact information, such as home address, email and telephone number;
- date of birth;
- gender identity and sexual orientation;
- race and ethnicity;
- employment and education history;
- background check information;
- citizenship status;
- marital and family status;
- identification documents, such as your passport, government identification number, or driver's license;
- banking information;
- emergency contact and beneficiary information;

- health-related information;
- job title, salary, workplace engagement, performance, disciplinary, and professional development information;
- time and attendance records;
- access card usage information (e.g., building entry and exit data);
- CCVS footage and other security-related data;
- occupancy data (e.g., workspace utilization and building capacity metrics); and
- other personal information you provide us or that we collect for purposes of establishing, managing, and administering our relationship with you and the work you perform for us.

How do we use your personal data?

We use personal data about you for purposes of establishing, managing, and administering our relationship with you and the work you perform for us. Some examples of how we may use your personal data include:

- workforce planning and recruitment, including business and space requirement forecasting, employee assignment planning, and budgeting;
- determining eligibility and suitability for initial and ongoing employment, including the verification of references and qualifications as part of a background check, aptitude and personality;
- administering all Human Resources (“HR”) policies and programs throughout employment, including managing talent, diversity and inclusion initiatives, employee engagement, learning and development, health and safety, evaluation of performance, compensation, benefits and promotion;
- performance of our business operations, including allowing us to work together and collaborate, to provide our services, ensuring business continuity, enforcing our rights and protecting our operations, and pursuing available remedies and limiting any damages we may sustain;
- legal and regulatory compliance, including ensuring compliance with health & safety requirements and legal or tax obligations, investigating or auditing compliance with our policies regarding anti-money laundering, bribery, and corruption, and responding to law enforcement requests; as required by applicable law, court order, or governmental regulations;
- if applicable, providing relocation support, which may include facilitating work permits or visas;
- acquiring and transferring our businesses;
- drawing insights from our employee data, to improve performance and culture;

- premises security management, including using access control systems and the use of CCVS cameras;
- information security management, including controlling access to information technologies and data and preventing cybersecurity breaches and data loss;
- investigating actual or potential incidents of error, fraud, security breaches, misconduct or other unlawful or harmful activities;
- performing functions required or authorized by law; and
- for any other purpose to which you consent.

How do we collect your personal data?

The personal data that we use generally comes from you. You provide us with your personal data when you complete forms, respond to our requests for information, participate in our surveys, or interact with our systems and processes. In some cases, the personal data we collect from you may be optional. If this is the case, we will let you know that you can decline to provide this information.

We may also collect personal data from third parties. For example, we may collect information from your public social media profile, recruiters, references, background check providers, third-party assessors in the event you have a disability and require accommodation, and other third parties that assist us in managing our HR needs or the benefits programs in which you participate.

If you provide us with personal data about another person, such as your beneficiary, you represent that you have all necessary authority and/or have obtained all necessary consents from that individual to enable us to collect, use and disclose that personal data.

What are our electronic monitoring practices?

We monitor OMERS facilities, networks, and assets (including mobile devices) in order to detect, prevent, and investigate error, fraud, or misconduct as well as threats to the security and operation of our IT systems and our data. This may include using technologies that profile user behaviour to identify unusual activity (such as logins from unexpected country locations) or to prevent data loss (such as export or email of data that is unusual or in violation of our policies).

Our acceptable use policies may permit limited and occasional use of OMERS facilities, networks and assets for personal purposes. Please check your OMERS group company policies. If you choose to use OMERS facilities, networks and assets for personal purposes, you should have no expectation of privacy since any such use will be monitored.

Electronic monitoring data is accessible to a limited number of authorized employees in our information technology and security teams. However, in the event of an investigation into a potential breach of our policies or other wrongdoing, electronic monitoring data may be accessed and used for the purposes of the investigation, including for disciplinary purposes up to and including termination for cause.

See Appendix 1 for further details on our electronic monitoring practices.

Is your personal data shared with third parties?

We may share your personal data with our affiliates and service providers who assist us with our business operations.

Below are some examples of third parties with whom we may share your personal information:

- information technology providers, such as cloud hosting services and software services;
- professional services providers, such as auditors, lawyers and consultants;
- recruitment services and background check providers;
- workforce planning and management service providers;
- services associated with corporate culture initiatives, including inclusion and diversity programs;
- survey, feedback and poll providers;
- data analytics service providers;
- employee coaching, training and education providers;
- travel and advisory services providers;
- expense recovery service providers;
- physical and digital safety and security service providers;
- collaboration technology service providers;
- global mobility and tax service providers;
- payroll providers;
- employee benefits providers (including employee health and wellness providers);
- your financial service providers such as your bank; and
- governmental agencies, such as national and regional tax authorities.

How do we draw insights from your personal data?

OMERS and certain third parties (including service providers and other third parties described in the section “Is your personal data shared with third parties?”) apply advanced analytical methods to derive insights that help improve HR operations and the employee experience. OMERS and these third parties may also de-identify personal information by removing identifiers and aggregating information about you with information about other employees. OMERS and these third parties may use this de-identified information for internal business purposes, including analytics, reporting, and workforce planning. In addition, OMERS or these third parties may anonymize personal information so that it can no longer be used to identify you. OMERS and these third parties may use and disclose anonymized information for any purpose, including sharing this information with additional third parties, as described in the section “Is your personal data shared with third parties?”.

Do we use artificial intelligence and machine learning tools?

OMERS and our service providers may incorporate artificial intelligence and machine learning tools to process your personal data, including to train and improve these technologies. These tools support internal business activities such as automating tasks, analyzing data, developing and improving HR initiatives, benefits, products or services, detecting fraud, protection systems, and other business purposes. OMERS is committed to using personal data responsibly and has internal processes to assess and oversee the use of these tools. This includes reviewing their purpose, the type of personal data used, the potential impact on your rights and freedoms, the risk of bias, and the extent of human oversight.

What about Cookies?

When you use our careers portals, we place files called “cookies” on your internet browser. These files ensure our websites function correctly during your visit and can also help our site remember any preferences you’ve set to assist you during future visits. Cookies used on OMERS websites also help us understand how our websites are used by visitors, including analyzing traffic trends, and how websites perform.

OMERS provides you with notice and choice over the cookies that are placed on your browsers. Upon a first visit to an OMERS website you will be presented with a banner that will allow you to set cookie preferences. The banner also provides you with more information on the specific cookies in use on our sites, which can be reviewed prior to setting preferences. You may update preferences at any time by navigating to the bottom of an OMERS web page and selecting the “Cookie Preferences” option.

Our websites may provide links to websites that are operated by third parties external to OMERS. This Privacy Statement does not describe the privacy policies of any third-party websites or their respective privacy practices. We are not responsible for how such third parties collect, use, or disclose personal data. When you visit a third-party site, you should familiarize yourself with their third-party privacy policies before providing those third-parties with your personal data.

How is your personal data kept safe?

Whether in electronic or paper-based format, we implement technical and organizational measures designed to provide an appropriate level of security, keeping in mind the nature, scope, context and purpose of processing, cost, and the potential risk to you. We use appropriate technology and efforts designed to safeguard your personal data from loss, theft, and unauthorized access, use or disclosure. We require our service providers and agents to protect personal data processed on our behalf.

Where is your personal data stored?

OMERS group companies operate in many countries, and we may need to transfer personal data to different countries to consolidate and centralize HR, D&T and other business functions, to improve efficiency by leveraging international expertise and technologies, and to facilitate collaboration among international teams. We and our service providers may transfer, store, or access personal data outside of the jurisdiction in which it has been collected, used or disclosed. Transfers of

personal data will be made in compliance with applicable data protection legislation and will only be made where there are suitable safeguards in place.

When a transfer takes place, personal data may be subject to the laws of those other jurisdictions, and in certain circumstances, the courts, law enforcement agencies, regulatory agencies or security authorities in those other jurisdictions may be entitled to access your personal data.

How can you access or correct your personal data?

You may have certain rights under applicable privacy laws, which can include the right to access, correct, or request deletion of your personal information, as well as other rights such as data portability or restriction of processing. These rights may vary depending on your jurisdiction and may be subject to legal limitations. Instructions for exercising these rights may be provided in specific portals or platforms. Current employees may submit a [Workday case](#). Former employees and applicants may e-mail a request to peopleexperience@omers.com.

We try to ensure that the personal data we collect about you is accurate, complete and up-to-date. However, we rely on you to provide accurate information in the first instance, and to notify us when there is a change in your personal data.

How long do we keep your personal data?

We retain personal data for only as long as it is needed to fulfill the identified purposes or as may be required to comply with applicable laws. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

How we update this Privacy Statement

As the law develops and as we evolve our operations, the way in which we collect, use, and disclose personal data may change. When this happens, we will update our Privacy Statement to reflect the changes. You can review our updated Privacy Statement at any time by visiting our website, <http://www.omers.com>, or by requesting a copy from our Privacy Officer.

Who can you contact with questions or concerns?

We have appointed a Privacy Officer who is responsible for overseeing our compliance with applicable privacy laws. If you have any comments or questions about our Privacy Statement, or if you believe that we have not complied with our Privacy Statement, please contact our Privacy Officer as follows:

Vice President, Privacy
900-100 Adelaide Street West
Toronto, ON M5H 0E2
Email: privacy@omers.com

SPECIAL NOTICE FOR RESIDENTS OF THE EUROPEAN ECONOMIC AREA AND/OR THE UNITED KINGDOM

As a resident of the European Economic Area and/ or the United Kingdom you are entitled to additional information about our data processing practices and you have additional privacy rights as set forth below. If you have questions about any of these rights please feel free to reach out to our Privacy Officer at privacy@omers.com.

Who is the controller of your personal data?

The controller of your personal information will vary according to the OMERS entity that employs you and your location. See the chart below to identify the controller responsible for your personal data.

| Corporate Employer | Region of Employment | Address of Corporate Office | Privacy Contact |
|---|----------------------|---|--|
| OMERS Europe Limited | UK | 122 Leadenhall Street, 29 th Floor, the Leadenhall Building, London UK EC3V 4AB | Vice President, Privacy privacy@Omers.com |
| OMERS Infrastructure Europe Limited | UK | 6 New Street Square, 12 th Floor, New Fetter Lane, London UK EC4A 3BF | Vice President, Privacy privacy@Omers.com |
| OMERS Infrastructure European Holdings B.V. | Netherlands | Muiderstraat 9U 1011 PZ Amsterdam, Netherlands | Vice President, Privacy privacy@Omers.com |
| OMERS Private Equity Europe Limited | UK | 122 Leadenhall Street, 29 th Floor, the Leadenhall Building, London, UK EC3V 4AB | Vice President, Privacy privacy@Omers.com |
| Oxford Properties Management (UK) Limited | UK | 122 Leadenhall Street, 29 th Floor, the Leadenhall Building, London, UK EC3V 4AB | Vice President, Privacy privacy@Omers.com |
| Oxford Properties Management (France) | France | 25 boulevard Malesherbes, 3 rd floor, 75008 Paris | Vice President, Privacy privacy@Omers.com |
| Oxford Properties Management (Germany) GmbH | Germany | c/o Greenberg Traurig Germany, LLP Potsdamer Platz 1 Berlin, Germany | Vice President, Privacy privacy@Omers.com |
| OPG Commercial RE Europe S.à.r.l. | Luxembourg | 6 rue Jean Monnet Luxembourg L— 2180 | Vice President, Privacy privacy@Omers.com |

What is the legal basis for our processing your personal data?

| Type of Personal Data | How we use it | Legal Basis for Processing |
|--|--|---|
| Basic contact information such as home address, email and telephone number | We use this information to communicate with you in connection with your employment. | The processing is necessary for our legitimate interests, namely in communicating with you with regard to your employment. |
| Demographic information such as date of birth and gender | We use this information to manage your employment relationship, including your access to benefits. We also use this information for demographic studies respecting the composition of our workforce. | The processing is necessary for the performance of a contract to which you are party, namely your employment contract and our obligation to provide you with access to benefits. The processing is necessary for our legitimate interests, namely understanding the demographics of our workforce. |
| Self-identification data such as gender identity, sexual orientation, race and ethnicity | We use this information to support diversity and inclusion initiatives aimed at improving our diversity and inclusion practices in the hiring process and throughout the employment life cycle. We also use this information to track our progress in this area and to report our progress for internal purposes and to comply with our regulatory reporting obligations. | You have provided us with explicit consent to process your personal data in support of diversity and inclusion initiatives. |
| Employment and education history | We use this information to determine your qualification for initial and ongoing employment and for development and promotion purposes. | You have provided us with your consent to process your personal data in relation to assessing qualification for employment. The processing is necessary for our legitimate interests, namely identifying suitable candidates for promotion, and management, and development of our workforce. |
| Background check information, including criminal offence data | We use this information to determine your eligibility for initial and ongoing employment and for compliance purposes. | You have provided us with your consent to process your personal data in relation to assessing your application for employment. The processing is necessary for compliance with a legal obligation to which we are subject, such as conducting background checks on regulated persons. |

| | | |
|--|---|---|
| | | The processing is necessary for our legitimate interest, namely ensuring the reliability and honesty of our workforce. |
| Citizenship status | We use this information to determine your eligibility for initial and ongoing employment. | The processing is necessary for compliance with a legal obligation to which we are subject, such as ensuring that you have a right to work in the jurisdiction in which you are applying. |
| Marital and family status | We use this information to administer our benefits program. | The processing is necessary for the performance of a contract to which you are party, namely your employment contract and our obligation to provide you and your beneficiaries with access to benefits. |
| Identification documents such as your passport, government identification number or drivers' license | <p>We use this information to identify you when necessary, to conduct background checks and to comply with know your client/anti-bribery and corruption/anti-money laundering and other compliance inquiries to which we are subject.</p> <p>We also use this information to set up your payroll account, to remit taxes on your behalf and to facilitate your employment where necessary such as assisting you in securing work permits or visas or travelling for your job.</p> | <p>The processing is necessary for compliance with a legal obligation to which we are subject, such as anti-bribery and corruption/ anti-money laundering requirements.</p> <p>The processing is necessary for our legitimate interests, namely responding to "Know Your Client" and corporate secretariat inquiries required for our business activities.</p> |
| Banking information | <p>We use this information to set up your payroll account.</p> <p>We also use this information to reimburse you for business expenses and expenses covered under your benefits program.</p> | The processing is necessary for the performance of a contract to which you are party, namely your employment contract and our obligation to pay your salary and to provide you with benefits. |
| Health and safety related information | <p>We use this information to facilitate payment of your benefits, to administer illness absences and other leaves of absence, to investigate workplace accidents or incidents, and to maintain a safe working environment.</p> <p>We also use this information to develop and administer employee wellness programs.</p> | <p>The processing is necessary for the performance of a contract to which you are party, namely your employment contract and our obligation to pay your salary and to provide you with benefits.</p> <p>The processing is necessary for compliance with a legal obligation to which we are subject, such as workplace safety regulation.</p> <p>The processing is necessary for our legitimate interests, namely supporting employee wellness in our organization and maintaining a safe working environment.</p> |

| | | |
|---|---|---|
| <p>Job title, salary, workplace engagement, performance and professional development information</p> | <p>We use this information to manage your employment, such as your remuneration, career growth and promotion.</p> <p>We also use this information for workforce planning purposes.</p> | <p>The processing is necessary for the performance of a contract to which you are party, namely your employment contract, and your eligibility to participate in incentive plans offered by OMERS, where applicable.</p> <p>The processing is necessary for our legitimate interests, namely identifying suitable candidates for promotion, and management, and development of our workforce.</p> |
| <p>Aptitude and personality surveys and tests</p> | <p>We use this information to evaluate suitability for roles, assist you in career development and for workforce planning purposes.</p> | <p>You have provided us with consent to process this information by participating in surveys and tests.</p> |
| <p>CCVS Camera Footage</p> | <p>We use this information to investigate or support the investigation of safety and security incidents at our offices.</p> | <p>The processing is necessary for our legitimate interests, namely the safety and security of our employees and visitors to our offices.</p> |
| <p>Information on external website usage, device details, transaction history and patterns</p> | <p>We use this information to improve your website experience and the website experience of other users, to understand how our websites are performing and to measure visitor traffic.</p> | <p>You have provided us with consent to process this information through preferences that you have selected on our Cookies Banner.</p> |
| <p>Information on the use of our information technologies, including company computers, phones, applications, intranet sites, and cloud-based services, including data associated with electronic monitoring activities outlined in Appendix 1.</p> | <p>We and our service providers use this information for the purposes outlined in Appendix 1 and to facilitate your access to these technologies, to secure these technologies and the data processed through them, to understand how these technologies are used, and to innovate.</p> | <p>The processing is necessary for our legitimate interests, namely the provision, management and security of these technologies and our data, the prevention of fraud or misconduct, and the management and improvement of our business.</p> |
| <p>De-identified, aggregated, or anonymized data</p> | <p>We or certain third parties (including service providers and other third parties described in the section “Is your personal data shared with third parties?”) may de-identify, aggregate or anonymize personal data and apply advanced analytics to derive insights for workforce planning, HR optimization, employee experience improvement and for our and our certain third parties internal business purposes.</p> | <p>The processing is necessary for our legitimate interests, namely improving operations and access to insights from certain third parties.</p> <p>We may also identify additional legal bases or provide you with notice of processing by those third parties as independent controllers.</p> |

What are your rights respecting your personal data?

In the EEA and the UK you have, subject to some legal limitations, the following rights respecting your personal data

- **Right of access.** You have the right to access and obtain a copy of your personal information.

- **Right of portability.** You have the right, in certain circumstances, to receive a copy of the personal information you have provided to us in a structured, commonly used, machine-readable format that supports re-use, or to request the transfer of your personal data to another person.
- **Right to rectification.** You have the right to obtain rectification of any inaccurate or incomplete personal information we hold about you without undue delay.
- **Right to erasure.** You have the right, in some circumstances, to require us to erase your personal information without undue delay if the continued processing of that personal information is not justified.
- **Right to restriction.** You have the right, in some circumstances, to require us to limit the purposes for which we process your personal information if the continued processing of the personal information in this way is not justified, such as where the accuracy of the personal information is contested by you.
- **Right to withdraw consent.** If we are processing your personal data based on your consent, you have the right to withdraw your consent from further processing.
- **Right to object.** You have a right to object to any processing based on our legitimate interests where there are grounds relating to your particular situation. There may be compelling reasons for continuing to process your personal information, and we will assess and inform you if that is the case. You can object to marketing activities for any reason.

If you would like to exercise any of these rights, contact our Privacy Officer at:

Vice President, Privacy
900-100 Adelaide Street West
Toronto, ON M5H 0E2
Email: privacy@omers.com

How do you file a complaint about our data processing?

If you have a complaint about our processing of your Personal Data you are entitled to file a complaint with the relevant Data Protection Authority.

Further information about how to contact your local data protection authority is available at [Complaints | European Data Protection Supervisor](#) . Residents in the UK may contact the Information Commissioner's Office: <https://ico.org.uk/>

SPECIAL NOTICE FOR RESIDENTS OF CALIFORNIA, USA

As a Resident of California, you are entitled to additional information about our data processing practices and you have additional privacy rights as set forth below. If you have questions about any of these rights, please feel free to reach out to our Privacy Officer at privacy@omers.com.

What personal information do we collect and how do we use it?

In the last twelve months we have collected the following categories of personal information:

- basic contact information, such as home address, email and telephone number;
- Protected Classification Characteristics, such as date of birth, gender, gender identity, sexual orientation, race and ethnicity;
- identifiers, such as your passport, government identification number or driver's license or utility bill;
- employment and education history;
- background check information;
- citizenship status;
- marital and family status;
- banking information;
- Emergency Contact and beneficiary information;
- health related information;
- job title and salary information;
- workplace engagement, performance and professional development information;
- photographic information, such as CCVS footage;
- website information, such as website usage, device details, transaction history, inferred geolocation and patterns of usage; and
- time and attendance records;
- access card usage information (e.g., building entry and exit data);
- CCVS footage and other security-related data;
- occupancy data (e.g., workspace utilization and building capacity metrics);and
- electronic monitoring information more fully described in Appendix 1.

What are our sources for personal information that we collect?

We may collect personal information from the following sources:

- directly from you;
- reputation and background check providers;
- our websites' data;
- data collected through our electronic monitoring activities; and,

- publicly available sources, such as social media applications.

What are our purposes for collecting, using and disclosing your personal information?

We may collect, use or disclose personal information about you for one or more of the following purposes:

- workforce planning and recruitment, including business and space requirement forecasting, employee assignment planning, and budgeting;
- determining eligibility and suitability for initial and ongoing employment, including the verification of references and qualifications as part of a background check, and aptitude and personality;
- administering all HR policies and programs throughout employment, including managing talent, diversity and inclusion initiatives, employee engagement, learning and development, health and safety, evaluation of performance, compensation, benefits and promotion;
- performance of our business operations, including allowing us to work together and collaborate, to provide our services, ensuring business continuity, enforcing our rights and protecting our operations, and pursuing available remedies and limiting any damages we may sustain;
- legal and regulatory compliance, including ensuring compliance with health & safety requirements and legal or tax obligations, investigating or auditing compliance with our policies regarding anti- money laundering, bribery, and corruption, and responding to law enforcement requests; as required by applicable law, court order, or governmental regulations;
- if applicable, providing relocation support, which may include facilitating work permits or visas;
- acquiring and transferring our businesses;
- protecting OMERS businesses against and investigating error, fraud, and misconduct;
- drawing insights from our employee data to improve performance and culture;
- premises security management, including using access control systems and the use of C CVS cameras;
- information security management, including controlling access to information technologies and data and preventing cybersecurity breaches and data loss;
- investigating actual or potential incidents of error, fraud, security breaches, and misconduct or other unlawful or harmful activities;
- performing functions required or authorized by law; and
- for any other purpose to which you consent.

What personal information have we disclosed about you in the last twelve months

In the past twelve months we have disclosed all of the categories of personal information listed in this Special Notice. The categories of third parties to whom we disclose your personal information for a business purpose are described in the General Privacy Statement in the question, "Is your personal information shared with third parties?"

We do not sell personal information to third parties for monetary or other valuable considerations.

What are your rights respecting your personal information?

As a resident of California you have, subject to some legal limitations, the following rights respecting your personal information:

- **The Right to Know.** The right to confirm whether we are processing personal information about you and, under California law only, to obtain certain personalized details about the personal information we have collected about you in the last 12 months, including:
 - the categories of personal information collected;
 - the categories of sources of the personal information;
 - the purposes for which the personal information were collected; and
 - the categories of personal information disclosed to third parties (if any), and the categories of recipients to whom the personal information were disclosed.
- **The Right to Access and Portability.** The right to obtain access to the personal information we have collected about you and, where required by law, the right to obtain a copy of the personal data in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.
- **The Right to Request Deletion.** The right to request the deletion of personal information that we have collected from you, subject to certain exceptions.
- **The Right to Correction.** The right to request that any inaccuracies in your personal information be corrected, taking into account the nature of the personal information and the purposes of the processing of your personal information.

We do not share personal information for cross behavioral advertising purposes or sell personal information.

You may have the right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights.

If you would like to exercise any of these rights, contact our Privacy Officer at:

Vice President, Privacy
900-100 Adelaide Street West
Toronto, ON M5H 0E2
Email: privacy@omers.com

Appendix 1 – Electronic Monitoring

| Tool | How | When | Purpose |
|--|---|---|---|
| Mobile device management | Monitoring mobile phones for information security, including IP location of access for unusual access location or if reported lost or stolen. | Continuous | Information security; Investigations. |
| Endpoint Detection and Response (EDR) | Monitoring the use of workstations (programs run, files read and written, etc.) and comparing it against a baseline to detect abnormalities and potential unauthorized uses. | Continuous | Network security; Information security; Investigations. |
| Access card | Monitoring physical access in and out of company premises. | When used | Physical security; Investigations; Attendance reporting; Space planning. |
| Virtual Private Network (VPN) Monitoring | Monitoring the network logins and the IP location of devices used by remote workers to access corporate networks. | When used | Information security; Investigations. |
| System Login Monitoring | Tracking login/logout of systems. | Intermittent (when logging in and out) | System security; Investigations. |
| Information Technology Usage Activity Monitoring | Tracking file upload or download on company devices; Tracking attempts to install non-approved applications on mobile devices. | Continuous (when used) | Network and system security; Investigations; Quality assurance and process improvement; understanding tool usage for business planning purposes. |
| Productivity and collaboration tools monitoring | Monitoring productivity and collaboration tools (including e-mail, calendaring, messaging, and virtual meeting platforms) to detect and prevent malicious activity or external attacks such as phishing and spam and to detect inappropriate behaviour. | Continuous (for user protection, acceptable use, and information security) Intermittent (for investigations and business continuity) | User protection; Monitoring acceptable use of company resources; Information security; Investigations; Business continuity (for example, after departure of an employee). |
| E-Mail and Message Archiving | For select segments of the employee population records are stored and maintained in Enterprise systems | Continuous | Legal compliance obligations. |
| Customer Service Technology Monitoring | Recording of interactions on customer service platforms. | Continuous | Quality assurance; Investigations. |
| Web Monitoring | Monitoring web browsing activities and monitoring requests to detect and protect against various known and unknown phishing malware, ransomware attacks. | Continuous | User protection; Monitoring acceptable use of company resources; Investigations. |

| | | | |
|---------------------------|--|--|--|
| Video Surveillance | Monitoring access to and occupancy of secure areas. | Continuous | Physical security; investigations; safety compliance. |
| Call Monitoring | Logging calls on company phone systems; recording calls in call centres. | Continuous | Quality assurance; sentiment analysis, compliance; investigations |
| GPS Location | Providing location-based services in certain business applications. | While location-based services are in use | Location-based services; physical security; investigations; safety compliance. |
| Space Utilization Sensors | Monitoring space utilization in company premises. | Continuous | Space planning. |