Privacy and cookies policy

This Privacy Notice may vary from time to time, so please check it regularly.

This Notice describes the types of information collected, how that information is used and disclosed, and how you can access, modify, or delete your information.

University of Plymouth Enterprise Limited (company number 03707827) whose registered office is at Finance Dept, Emdeck Building, Plymouth, Devon, PL4 8AA ("we", "us" or "our") is the 'data controller' for the personal data we collect. We are registered with the Information Commissioner's Office with registration number Z2829314.

1. Marketing, analytics and guest services

How do we collect information about you?

1. Sign in: We will collect personal information on you when you use our Centre Sign In facilities such as full name, visiting company name and vehicle registration.

2. Feedback: provide feedback to us through our online surveys, where you may provide your contact details and subscribe to receiving marketing information. You can also provide us with feedback through writing to or emailing the centre with any comments, complaints, or suggestions.

3. Website usage: We may also collect information from you automatically when you access and use our Online Services, including the time and duration of your visit, the referring URL, your Internet Protocol (IP) or MAC address, the type of device you use and its operating system. As with most websites, we operate cookies on ours, and further details can be found in the section on cookies below. We use non-essential cookies (including analytics and tracking cookies) only with your explicit consent, in accordance with UK GDPR and PECR requirements.

4. Enrolling for an event or making a booking: We may collect your name, email address, company name and other contact details when you register for an event or make a room or resource booking at one of our centres. This data is processed via Nexudus Spaces, an online workspace and events management platform operated by Néxudus Ltd. (Company No. 09772435), which acts as a data processor on our behalf under a contractual agreement. When you create an account directly with Nexudus Spaces, Néxudus Ltd. also acts as an independent data controller for your account credentials and platform usage data. We recommend reviewing their privacy policy at nexudus.com before registering. We use this information solely to manage bookings, confirm registrations, process payments and communicate event details with you.

5. Promotional Photography or Filming: We may take photographs or video of you when you attend one of our events. If you have concerns or do not wish to be photographed or filmed, please raise these with a member of our staff. These images will be used for promotional purposes on our website and social media unless you've explicitly notified us in writing that you do not wish us to use your image for such purposes.

6. Interaction with social media: depending on the Privacy setting you have applied to your social media accounts and based on the content that you choose to share, when you interact with our Social Media presence, we will have access to your user-generated content, such as posts, comments, pages, profiles and images. Also, depending on the Privacy setting you have applied in your Social Media accounts, and based on the content that you choose to share, we may have access to contact details, personal information (such as age, gender, employer, education, location and habits and preferences).

7. Car parking: we may collect your registration number as a key identifier to process vehicles. The purpose is to plot the vehicle movements, apply fees and membership etc. Your credit/debit card details will be collected if you choose this payment method. Our payment providers and operators of our Car parking services are third parties. We use FxPlus as car parking operators and therefore processors of this data. We use Newpark Security Limited payment processors and Global Payment's merchant banking services.

8. Loan or hire equipment: you may provide us with your personal details so that we can loan or hire equipment to you, such as office equipment, furniture or moving/handling equipment.

9. Miscellaneous Forms: there are miscellaneous forms at the site which can also record your personal information – for example, induction, lost property, incident reports, event/room booking etc.

10. Postal Service: We may provide a service to distribute mail to you at our site and we will use your contact details on our mailing system to notify you.

11. Access Control: We may ask you for an email address and a photo from which a biometric file of you will be created should you wish to participate in face-recognition access control systems at one of our centres. This data may be captured and maintained by third parties. Privacy policy found here. Participation in facial recognition is entirely voluntary, and a non-biometric alternative (e.g., access card) is always available. Biometric processing is special category data under Article 9, and we rely on explicit consent for this purpose.

Lawful Basis

In all the above instances, we will only provide you with email marketing where you have consented, and you can withdraw this consent at any time by clicking the unsubscribe link within the emails you receive or by emailing Reception with your request.

We may also use third-party PR/marketing agencies who may have access to your personal details to develop email PR/marketing campaigns and social media, to provide customer insight through the analysis of data and to collect personal data on our behalf.

For social media, our purpose is to serve our legitimate interests to

i) respond to customer complaints.
ii) obtain insight into the use and perception of our customer offerings so that we can improve them. For example, we collect and analyse the public posts that you make directly to us on social media to help us understand if we are receiving negative or positive comments across all our social media channels)
iii) Run promotions, competitions and events to increase engagement with our customers. License plate data is also collected for our legitimate interest to understand how the car park is used to optimise the customer experience.

Where processing involves special category data (e.g., biometrics), we rely on explicit consent (Art. 9(2)(a)) or, where appropriate, substantial public interest for safety and security purposes.

Data minimisation and retention

We will only collect the minimum amount of personal information necessary and will only keep your information for as long as you remain engaged with our Centres. Where you unsubscribe from our marketing, we will add your email address to our suppression list and delete any additional information that we hold about you.

For Sign in/out purposes, your personal data will be held for 12 months and then deleted from our system.

For analysing responses to customer feedback, we generally keep these for 15 months to allow year on year comparisons.

Images of vehicles are deleted after 90 days and vehicle movement information, violations and debug logs are deleted after 12 months.

2. Security

How do we collect information from you?

As part of our security operation, we will also be collecting personal images relating to visitors and customers to its properties from CCTV, ANPR (Automatic Number Plate Recognition) and for the optional use of facial recognition systems.

We use third-party service partners to provide security services, and information recorded through these technologies is held on systems maintained by them. The data we collect may be shared with the police, customers, local authorities, other sites or local crime-reduction partnerships and initiatives for our legitimate interests to run successful businesses in environments that are safe for our staff and customers, and for the prevention and detection of crime. These organisations may also share data with us. ANPR data can be shared with third parties for enforcement purposes.

We may also obtain and share the information with insurance companies where they request data relating to insurance claims to support their legitimate interests, or those of their clients, or to defend legal claims.

We also capture personal data within Access Control. Personal data is also collected from visitors to our properties. Access control data is held within our systems but may be maintained by third parties and the visitor management data may be held on third-party systems.

In relation to access control and visitor data, where the data relates to our employees, contractors or visitors, we consider ourselves to be the Data Controller. For personal data relating to our occupiers' staff and employees, we also consider ourselves to be the Data Controller. Our sites use systems hosted by third parties to register visitors and, if relevant to the site, collect facial recognition information for which they are considered the controller. This data is used by our reception to provide access to the building.

In relation to Mail Handling, We may receive physical mail addressed to customer businesses for the purpose of internal redistribution. We act as Data Processor when receiving physical mail and placing it into the customer's assigned mailbox or collection point. We do not determine the purpose or means of processing, and we do not access the data contained inside.

The customer (licensee) is the Data Controller for the personal data contained within their mail.

Security Analytics: Our CCTV may use technology that detects when a person is present and raises an alert based on their location, such as someone being in the building after closing or in a restricted area. On-site or security staff will attend to these alerts to decide on the appropriate action. This technology supports University of Plymouth Enterprise Limited in maintaining site security and safety as a legitimate interest. Where applicable, it may include facial recognition for biometric identification.

In relation to third parties, we ensure that they will also safeguard your data – please see Protection of Your Information below.

Our CCTV systems do not record audio.

We have identified all third-party processors supporting CCTV, ANPR and access-control systems, and details of relevant categories of recipients are included within this policy (see Section 5).

For what purpose is it collected?

CCTV, ANPR, Visitor and Access control data is collated to pursue our legitimate interests to protect the property in question, to protect the safety and vital interests of our visitors, employees and customers, to assist with the prevention and detection of crime and to provide our contracted service to our customers. CCTV is not used for monitoring of staff or customers or contractual performance; however, if CCTV is required as part of a disciplinary investigation, it can be used for this purpose if the seriousness of the investigation warrants it.

ANPR is collected to fulfil a contract between the users of our parking facilities, including enforcement action and Us.

Access control data is processed because of our contractual responsibilities to our occupiers.

We process mail solely to:
- receive items addressed to customers
- ensure they are distributed securely to the customer's mailbox or collection point
- notify customers of oversized items held for collection

We do this to fulfil our operational responsibilities in providing managed workspace and to maintain the safety and security of the building. This aligns with our legitimate interests as described in Sections 2 and 5 of this Privacy Policy.

Where biometric data (facial recognition) is used for access control or identity verification, this constitutes special category data. Processing is based on explicit consent under Article 9(2)(a), and participation is always optional with alternative access methods provided.

A Data Protection Impact Assessment (DPIA) has been completed for the deployment of biometric, as required by UK GDPR.

Where ANPR or security-analytics systems trigger alerts or recommended actions, these are always reviewed by a human operator, and no decisions with legal or significant effect are made solely by automated means.

Data minimisation and retention

For CCTV: Generally, this data will not be held for longer than 31 days unless an incident or suspected incident has occurred.

ANPR: Images of vehicles are deleted after 90 days and vehicle movement information, violations and debug logs are deleted after 12 months.

Access Control Systems: Access provided by card or facial recognition and the personal data associated with them will be deleted on a user's last day or by request from a business manager. Access data will be purged from the system after 24 months. Any passes which have remained inactive for twelve months will have all data relating to the card permanently deleted.

Visitor Management Systems: All data is deleted from our system after 12 months.

For event and booking data held within Nexudus Spaces, personal data will be deleted within 30 days of the cessation of services or upon your request, in line with Néxudus Ltd.'s data retention policy.

Retention periods for biometric templates follow the same principle: biometric files are deleted immediately upon withdrawal of consent or cessation of building access.

3. Accident and incident reporting

How do we collect information from you?

When an incident occurs at one of our properties, we are required to document the particulars of an incident which may include witness statements, CCTV footage, photographs and written reports. This information may include special categories of data depending on the nature of the incident. A third-party system is used to log details relating to these incidents and physical paperwork may also be stored on site.

Where an incident concerns personal data contained inside the mail, responsibility for assessment and reporting remains with the Data Controller (the customer or original sender).

The data may be shared with third parties such as insurance providers and legal advisors to defend a claim, government or other competent organisations who are required to report on incidents by law or the police to investigate a crime. It may also be shared with a third party who are liable for a claim under their contractual relationships with us for the purposes of allowing them to defend a claim. This information may also be shared with government or other competent organisations who are required to report on incidents by law or the police to investigate a crime.

Where incident-related CCTV includes enhanced analytics, security alerts or biometric identification (where applicable), we confirm that these elements are always reviewed by a human operator and are not used to make solely automated decisions that produce legal or significant effects

For what purpose is it collected?

This information is collected to ensure that we comply with our legal responsibilities in relation to Health and Safety investigation and reporting, and in relation to any future legal claims. The information can also be used to prevent and detect crime or to protect the vital interests of individuals. Where health information is collected, we may also need this for our substantial public interest for Insurance processing.

Where special category data is processed as part of accident and incident reporting (for example, health data or biometric data included within CCTV footage), the lawful basis under Article 9 will be substantial public interest or establishment, exercise or defence of legal claims, depending on the scenario.

Data minimisation and retention

All personal data (CCTV, witness statements, photographs and written reports) relating to an incident is held for six years, unless there are reasons to retain it for longer, such as an ongoing HSE investigation, a suspected pattern of fraud, or because an injury has been sustained by a child.

We do not retain copies of mail or record the content of envelopes.
Associated operational logs are retained in accordance with:

- incident reporting retention (six years)
- CCTV retention (31 days unless extended for investigation)
- visitor and access control retention periods described in Sections 2 and 3

4. Other uses

In addition to the purposes already described, we may use information collected to perform other important business operations, for example: to understand usage patterns (such as foot traffic) within our properties; to develop, provide, improve and personalise products and services; and to provide customer service/support. We may undertake additional research, analysis, and surveys, both online and in our centres. The lawful basis for this use of Information is for our legitimate business interests.

5. Other recipients and third-party transfers not detailed previously

We may pass on or allow access to your information:

- to our suppliers, contractors and professional advisors where this is necessary for them to provide services and facilities to us, such as to provide car parking, access or maintenance services.
- to any purchaser of all or part of our business or any of our properties;
- to sell, make ready for sale, or dispose of our business wholly or partly, including to any potential buyer or their advisers;
- where we are required to do so by law, court order or other legal process;
- where, acting in good faith, we believe disclosure is necessary to assist in the investigation or reporting of suspected illegal or other wrongful activity. This may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction; to protect and defend our rights or property; to deal with any misuse of any of our Services; or to enforce or apply our terms and conditions and other agreements with third parties.
- to our group companies and affiliates or third-party data processors who may process data on our behalf to enable us to carry out our usual business practices.
- We use Néxudus Ltd. as our events and workspace booking platform. Data processed through this system may be stored and transferred between countries in which Néxudus operates.
- University of Plymouth Enterprise Limited uses Microsoft Office 365 cloud technology for its operations. Its data centres are located within the EEA.

6. Protection of your information

We have in place administrative, technical and physical measures designed to guard against and minimise the risk of loss, misuse or unauthorised processing or disclosure of the personal information that we hold. We place similar obligations on our third parties and risk assess their security based on the sensitivity of the personal data that they hold.

If we transfer your personal information outside of the UK, it will continue to be subject to one or more appropriate safeguards set out in the law. These might be the use of model contracts in a form approved by regulators, or having our suppliers sign up to an independent privacy scheme approved by regulators.

Where a breach may meet the threshold for notification, we will report it to the Information Commissioner's Office (ICO) without undue delay, and within 72 hours where legally required.

If a personal-data breach creates a high risk to your rights and freedoms, we will notify you directly in accordance with our legal obligations.

7. Links to other websites

This Privacy Notice only applies to the websites or systems provided or maintained by us. If you link to another service and/or website not maintained by us, you should remember to read and understand that service and/or website's privacy and cookies policy as well. We are not responsible for any use of your information that is made by other services and/or websites. Links or advertisements do not imply that we endorse or have reviewed such third parties or their privacy practices.

Where we include links to third-party websites or services, we do not control and are not responsible for how those third parties collect or use your personal data. We recommend reviewing their privacy information before providing any personal data or accepting cookies.

If a third-party service collects personal data directly from you (for example, event-booking platforms, payment gateways, or social-media platforms), they act as an independent Data Controller for that processing. We do not receive all of the data you provide to such services, and any data sharing between those providers and us is limited to what is necessary for the specific purpose (e.g., booking confirmations or payment reconciliation).

8. Your rights

You have the right to opt out of receiving any marketing information which we send you.

Your duty to inform us of changes.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the following rights:

- Subject to certain conditions, request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. If possible, you should specify the type of information you would like to see to ensure that our disclosure meets your expectations. Disclosure should not impact the rights and freedoms of other people, e.g., the privacy and confidentiality rights of others.
- Subject to certain conditions, request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. You also have a responsibility to help us to keep your personal information accurate and up to date.
- Subject to certain conditions, request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. We may be unable to erase some information where we must retain it to comply with legal obligations or defend legal claims.
- Subject to certain conditions, you may object to the processing of your personal information where we rely on legitimate interests and something about your situation triggers this right. You also have an unconditional right to object to direct-marketing processing.
- Subject to certain conditions, request restriction of processing—for example, while accuracy is being verified or where processing is being contested.
- Subject to certain conditions, request the transfer of your personal information to another party. This applies where processing is based on consent or contract and is carried out by automated means.
- Where processing of your personal data is based on your consent, you have the right to withdraw at any time. If you do decide to withdraw your consent, we will stop processing your data for that purpose, unless there is a lawful basis we can rely on – in which case, we will let you know. If you withdraw your consent, this will only take effect for future processing.

If you want to review, verify, correct, or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please email one of the email addresses below.

We aim to respond to all valid rights requests within one month. Where requests are complex or numerous, we may extend this timeframe by a further two months, but we will always inform you if an extension is required.

You will not normally have to pay a fee to access your personal information or exercise any rights. However, we may charge a reasonable fee or refuse to comply if a request is unfounded, repetitive or excessive.

You can contact the Information Commissioner's Office via https://ico.org.uk/ for information, advice or to make a complaint.

What we may need from you

We may need to request specific information to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is a security measure to ensure that personal information is not disclosed to anyone who has no right to receive it.

If you wish to opt out of marketing, please contact:

Centre	Email
Pool Innovation Centre	Lorna.sutton@plymouth.ac.uk
Tremough Innovation Centre	Helen.bush@plymouth.ac.uk
Health & Wellbeing Innovation Centre	Bethany.winnan@plymouth.ac.uk

9. How do we use cookies?

In our website we use cookies to collect information of how many visitors there are to different parts of the website, which helps us keep our site up to date. We may also use cookies to tailor the content that you see to suit your interests. This facility also allows you to receive personalised advertising relating to products viewed whilst using our website.

Strictly Necessary Cookies

Required for the website to work. These cannot be switched off and do not store personal information.

Performance Cookies

Help us understand website usage (e.g., most-visited pages).
Only active if you have opted-in.

Functional Cookies

Remember the choices you make and enable enhanced website features.
Some may be set by third-party service providers (e.g., embedded tools).

Targeting Cookies

Support personalised advertising and measure campaign effectiveness.
Only set with your explicit consent.

10. Changes to the privacy & cookies policy

This Privacy Notice was last updated on 30th March 2026. If it is necessary for us to alter the terms of the Privacy Notice, we will post the revised Privacy Notice here. We encourage you to frequently review the Privacy Notice for the latest information on our privacy practices.

Where changes to this Privacy Notice involve significant updates to how we process personal data, we will take appropriate steps to notify you. This may include email notification, on-site signage, system notifications, or notices published on our website.

Where a change relates to processing based on consent, we will request renewed consent if the nature of the processing changes in a way that requires it.

We maintain version control and a documented revision history to ensure that all updates to this Notice remain transparent and traceable.

Document Review History

Version No.	Date of Change	Originator of Change	Description of Change
001	04/06/2023	Sharna Devine-Forbes	Document created
002	23/05/2024	Sharna Devine-Forbes	Included references to facial recognition in sections 1.11, 2, 4 & 7
003	23/01/2026	Sharna Devine-Forbes	Includes addition of mail handling in sections 2 and 3; Inclusion in section 1.5 of need for written notice not to use promotional photography or filming on website/social media
004	30/03/2026	Sharna Devine-Forbes	Added required GDPR transparency updates, including lawful-basis clarifications; consent requirements for biometrics and cookies; automated-decision-making information; updated third-party transparency; retention-schedule enhancements; and improvements to rights-handling guidance.
005	05/05/2026	Sharna Devine-Forbes	Expanded section 1.4 following the implementation of a new Event booking system. Included Nexudus in the list of suppliers. Updated data minimisation section to include Nexudus data holding policy.