

Biometric Policy

Reviewed: August 2025

Summary

We use a secure facial recognition system to manage safe access to the Integrated Centre, Nursery, Couthie and Research & Training Base. Biometric data is stored in Microsoft Dynamics 365 within the UK and European Economic Area (EEA), ensuring full protection under UK GDPR and EU GDPR standards. Access is restricted to authorised staff only, and all data is encrypted, password-protected, and deleted when no longer needed. Parents, carers, and students must give consent to register and may withdraw it at any time by contacting the Head of Centre at angela.prodger@pengreen.org. An escorted entry option is available for those who do not consent. Staff are required to use the system. The system helps ensure safeguarding, accurate fire safety checks, and secure entry across the site.

Biometric data relates to personal data resulting from specific technical processing of the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial imagery.

This policy primarily relates to the use of facial recognition technology across the Integrated Centre, with one exception: a fingerprint reader is used in the Research, Training and Development Base to support security alongside facial recognition.

The facial image is classed as biometric data and the Integrated Centre must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018. Where the data is used as part of an automated biometric recognition the Integrated Centre must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act (2012).

Facial recognition System Process

To ensure the safety and well-being of all in the Integrated Centre the following processes are undertaken:

- Facial images are required for all parents and carers to access their child's specific setting. Parents and carers will only have access to that particular setting. If parents and carers have more than one child attending the Centre at any one time they will have access to the relevant settings in which their children attend. This will allow the parent/carer to only access the area for which their child attends. The only exception is for children attending a late session and for which they are located in a different area.

Parents/carers will have access to those areas that their child may be located within at the end of the day.

At any point during the academic year that a child leaves the setting then all personal data for parents and carers relating to system registration and facial imagery are deleted immediately.

- Staff and Volunteers on placement within the Integrated Centre are required to register their images in order to enter, and leave, the building. At the end of placement and/or when a member of staff leaves the organisation all access rights are removed and personal data relating to facial imagery are deleted. Staff biometric data may also be used for HR management functions.
- Students attending the Research & Training Base are required to register their facial image or fingerprint in order to enter and leave the building. Biometric data of students attending block weeks of study is kept only for the duration of their studies and removed at the end of their study block.
- Consultants working within the Research & Training Base will need to register their facial image or fingerprint for the period they are engaged to deliver consultancy work. On completion, their details and access rights will be removed.
- All visitors and external contractors visiting the site will be escorted by the appropriate member of staff in order to access the required areas and will not be left unsupervised.
- Authorised Governors use the Biometric system.
- If someone has a specific need or disability which prevents them from accessing the facial recognition system, they will be escorted to and from their destination.

Registration for the system is undertaken at the Main Reception for all individuals accessing the main building. Registration for the Research & Training Base is undertaken at the Research Reception.

For Health & Safety purposes each individual registered on the system is required to log their image on each occasion of entering and leaving the building. The practice of tailgating is not permissible given the system is used within emergency situations to accurately check the location of individuals across the whole site at any given time, for example during fire evacuation procedures. In addition, there is the facility on the system to lock down specific areas of the building and the system is used again to check the location of individuals and to ensure the safety of all across the Integrated Centre.

Storage and Access

All biometric data is stored securely within Microsoft Dynamics 365, which includes robust security protocols such as encryption and password protection. Data will only ever be stored or transferred within the United Kingdom and the European

Economic Area (EEA), which ensures that all personal data is fully protected under the requirements of the UK GDPR and EU GDPR, or equivalent legal standards.

Access to the system is strictly controlled and limited to the following roles:

- Receptionists (Pen Green Centre & Research): ability to register individuals.
- Pen Green Centre Administrators, Executive Assistant & Marketing Officer (Research Base): ability to register and manage changes within the system (e.g. children changing settings, deletion of leavers).
- Head of Centre: all of the above functions and, in addition, the ability to 'lock down' areas of the building across the whole site.

The machines used in the daily function of the system are password-protected and stored securely when not in use. The Head of Centre can also access the system from a work laptop in order to block access or initiate a lockdown process remotely if required.

For Health & Safety purposes, each registered individual must log their entry and exit to the building. This ensures accurate records of who is on site in emergency situations such as fire evacuations. Tailgating is not permissible, as the system is used to verify the presence and location of individuals across the site.

Consent to use the system can be withdrawn at any time by parents, carers, or students by contacting the Head of Centre at angela.prodger@pengreen.org. If consent is withdrawn, their biometric information will be deleted from the system and access will be managed by escorted entry. Staff are required to use the biometric system to access and leave the building.

As stated elsewhere, when a child, student, or member of staff leaves the Centre, all personal data relating to their biometric registration is deleted. The only exception is where a younger sibling continues to attend, in which case the parent/carer's access remains active.

Digital Face Recognition

In addition to the biometric access system, the Integrated Centre uses digital photography of children for marketing and communication purposes. This is managed in line with the Online Security Policy and subject to explicit parental consent.

Digital images are stored securely on two password-protected Apple Mac computers used by the Marketing and Communications Team. These devices are connected via a secure, encrypted cloud-based system, allowing images to be shared between them. Access is restricted to two authorised staff members only.

Apple Photos facial recognition software is used solely to:

- Organise and categorise images, and
- Cross-check that valid parental consent has been given and remains current.

Images are stored for a maximum of **three years** from creation, in line with the Online Security Policy. At the end of this period, or when parental consent expires, images are permanently deleted.

The only exception is where **additional, specific parental consent** has been granted for longer retention. This applies in cases where images are incorporated into research projects, training materials, or published educational resources.