ievo®

RELIABLE. BIOMETRIC. SOLUTIONS.

Securing Nurseries

Statutory requirements: "Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare." - HM Government document 'Working together to safeguard children'.

ievo Ltd understand the requirements set out by the UK Government and Ofsted in order to protect and safeguard children. In order to protect those in their younger years, **ievo** Ltd provide biometric systems to protect and improve safety measures in nurseries.

SECURING YOUR ENVIRONMENT

One of the key features of outstanding practice according to Ofsted is: "robust arrangements for site security, understood and applied by staff and pupils". Taking this on board **ievo** Ltd understand that nurseries need to protect children and staff members and offer parents piece of mind that their children are safe in a protected environment while out of their care.

ievo Ltd biometric solutions provide a safe and secure environment by utilising fingerprint recognition technology to govern access. As fingerprints are developed as an individual grows, children of a young age* may not process enough identifiable data points on their fingerprint to use such a system, therefore **ievo** systems are recommended to be used to control access for staff members and parents, ensuring that only those who are registered are allowed access. The control access system will provide a safe and secure environment for safeguard younger children in the early years of education and development.

INNOVATIVE TECHNOLOGY

High levels of security are a vital concern to parents and can be a deciding factor when choosing a nursery or childcare centre, likewise knowing which system to install is vital for staff to understand. **ievo**'s innovative technology seamlessly integrates into new or existing security systems allowing for flexibility in installation.

When registering a fingerprint with **ievo** devices, the reader will send an image of the fingerprint to an **ievo** control board where an advanced algorithm will extract and convert key data using a unique proprietary template format which is then stored in a database on the control board. The template can then be used for identification purposes when using the system, which will only grant access to registered users, protecting and securing those within. The original fingerprint image is not stored or recorded and no data is stored on the **ievo** reader unit.

ACCESS CONTROL

Controlled security is paramount in providing a safe environment for children and staff. Knowing who has access and when is vital in maintaining a safety net. Biometric identification supports a high level of security and **ievo** fingerprint readers are designed to integrate into access control systems by adding an additional layer of security to an infrastructure.
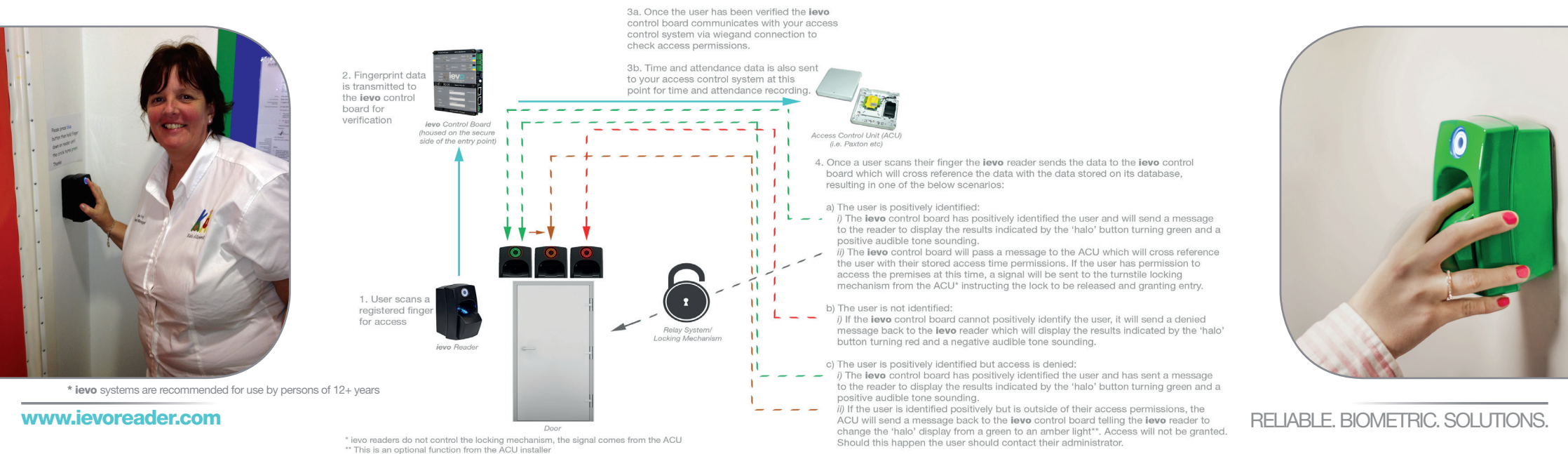
SYSTEM INTEGRATION

ievo systems work with a number of well-known access control systems, including; Paxton, Stanley, Honeywell and Nortech, to adhere to the Ofsted mission of safeguarding children. The seamless integration allows for interaction between systems, improving safety measures and reducing costs for installation.

CONTROLLED ACCESS

ievo's biometric readers removes any potential vulnerabilities of card, fobs/token systems, by giving control back to the system. Only a registered fingerprints will be able to access the facility. To be in line with best practice however, **ievo** solutions can be installed with a card reader function which will accept some card systems, allowing duel access for staff or parents who do not wish to use biometric data, but still safeguarding them under the same security measures.

BESPOKE SOLUTIONS: IEVO PRODUCTS

ievo biometric readers can be installed in a variety of ways, with either just main entrance points with one reader, or a system of multiple readers installed throughout a facility. Systems can be installed with a mix of **ievo** biometric readers within one system. Different access rights can be given to different users via an access control system, allowing, for example, only staff to access staff only areas, e.g. supply rooms or facility management areas. Aside for the technical aspects of **ievo** devices, the **ievo** readers can be provided in custom colours, ensuring that your systems blends in with your environment.

3a. Once the user has been verified the **ievo** control board communicates with your access control system via wiegand connection to check access permissions.

3b. Time and attendance data is also sent to your access control system at this point for time and attendance recording.

2. Fingerprint data is transmitted to the **ievo** control board for verification

ievo Control Board (housed on the secure side of the entry point)

Access Control Unit (ACU) (i.e. Paxton etc)

4. Once a user scans their finger the **ievo** reader sends the data to the **ievo** control board which will cross reference the data with the data stored on its database, resulting in one of the below scenarios:

a) The user is positively identified:
   i) The **ievo** control board has positively identified the user and will send a message to the reader to display the results indicated by the 'halo' button turning green and a positive audible tone sounding.
   ii) The **ievo** control board will pass a message to the ACU which will cross reference the user with their stored access time permissions. If the user has permission to access the premises at this time, a signal will be sent to the turnstile locking mechanism from the ACU* instructing the lock to be released and granting entry.

b) The user is not identified:
   i) If the **ievo** control board cannot positively identify the user, it will send a denied message back to the **ievo** reader which will display the results indicated by the 'halo' button turning red and a negative audible tone sounding.

c) The user is positively identified but access is denied:
   i) The **ievo** control board has positively identified the user and has sent a message to the reader to display the results indicated by the 'halo' button turning green and a positive audible tone sounding.
   ii) If the user is identified positively but is outside of their access permissions, the ACU will send a message back to the **ievo** control board telling the **ievo** reader to change the 'halo' display from a green to an amber light**. Access will not be granted. Should this happen the user should contact their administrator.

1. User scans a registered finger for access

ievo Reader

Relay System/ Locking Mechanism

Door

* ievo readers do not control the locking mechanism, the signal comes from the ACU
** This is an optional function from the ACU installer

* **ievo** systems are recommended for use by persons of 12+ years

RELIABLE. BIOMETRIC. SOLUTIONS.

KEY BENEFITS OF IEVO SYSTEMS

- Safeguarding children, staff and parents
- Simple and highly effective solutions
- Cost effective
- Improved health and safety records
- Integrated system to work with your infrastructure
- Future proof design - for any future upgrading or additional development of your security system
- Full customisable and serviceable up to and after the point of sale
- Customisable colours to discreetly blend into your environment

ievo Ltd is a leading design and manufacturer of biometric fingerprint readers. Working with a number of installers and integrators, **ievo** Ltd have a proven track record securing food and drink manufacturing facilities worldwide.

For case studies or further information, please contact our support team:

info@ievoreader.com
Tel: 0845 643 6632 / +44 (0) 191 296 3623
or visit:
www.ievoreader.com