March 2021

Cashless Catering and the use of Biometric Technology at King Edward VI Community College

These notes provide information about the use of the biometric technology system for cashless catering. In producing this, we have recognised the advice from BECTA (the Government agency leading the national drive to ensure the effective and innovative use of technology throughout learning) and the ICO (Information Commissioner's Office – which is responsible for regulating and enforcing the access to and use of personal information). It covers the following:

1. **An explanation of how it works**
2. **The advantages**
3. **Registration & Consent**
4. **Information and reassurance about how personal data is used and kept safe**

1. Explanation of cashless catering and Biometric Technology – how it works

What is a cashless system? A cashless system is used for the payment of school meals, where no cash is taken at the point of sale. Each student and member of staff using the system will be allocated an account, much like a bank account. This information is held on a secure server and stores details of individual cash balances, records cash spent and cash received, records where money has been spent, on what food and the exact date and time the money was spent.

How are students and staff recognised by the system? Prior to the system going live, all individuals intending to use the system will have their finger scanned. This finger scan will be converted into a number and stored on the system against that individual. Once the finger scan has been taken, it is automatically converted to numeric form. No register of fingerprints is kept and it is impossible to reconstitute a fingerprint from the numeric reference.

How is the biometric recognition system used to obtain a meal? At the till point is a dermal scanner. When the student wishes to pay for a meal, they simply place their thumb/finger on the scanner; this will bring up that individual's account. A display will show the terminal operator the student's name, tutor group and current cash balance held within the system. The selected food items will be entered into the system from the touch screen terminal while the product values and the total balance will show on the display.

How is money entered into the system?
(a) By an online payment engine – the secure online payment facility available through the school's Parent App (you will be sent details of how to log on to this separately. **Payments made via Parent Pay must be allocated to Catering**.

(b) By Cash (notes/coins) into Revaluation Unit located in the Redworth Dining Room.

How does the revaluation unit work? Firstly, the student places their thumb/finger on the scanner mounted on the Revaluation Unit. The system will identify the individual and display their name and current cash balance held within the system. Next, coins/notes are inserted into the slot. Each incremental cash balance will show on the display. Simply press the green lit button to complete the transaction.

How can you check your current balance held on the system? By using the Revaluation Unit, simply access your account by placing your thumb/finger on the scanner or by entering your PIN; there is no need to deposit any money. Your details will show on screen and then press the green button when finished. You can also view your balance through the Parent App by going to the Payments section.

If we pay for a set number of school meals, can it be spent in one day? On request, the caterers (Aspens Services) can set up individual spending limits for students.

How does the system deal with students entitled to free school meals? The system works exactly the same for all students, whether they pay or have a free school meal entitlement. The amount allocated for the free school meal will be entered into the system by the software daily and will only be accessible at break-time and lunch break.

The system will then allow, on a daily basis, the required cash amount for each individual student to be allotted to their current cash balance. However, any under-spend or missed dinner will be identified by the system and *will not* be added to the next day's balance. The student can also add extra cash onto his or her balance in the system by using the Revaluation Unit, to enable a greater daily spend on the school dinner than allocated by their free meal allowance. As this allowance can only be spent on a school dinner, extra cash added into the system can also be used for breakfast or break time snacks. All students in receipt of this benefit will retain complete anonymity.

Will we be able to have any information on how the system is being used? Should they so wish, parents have the ability when on-line to access their child's account(s) and view what meals are being taken and what food money is being spent on. This is particularly useful for budgeting purposes or in case of any dietary restrictions. Both credits and debits to the account (s) can also be viewed along with current balances (money available to spend).

Biometric Registration: Each individual's finger and thumb prints are unique. The Biometric cashless system will store only a section of the print as a unique number and not as an image. Each child will have that unique number stored on a central server. This is done by scanning the finger or thumb with a non-evasive electronic scanner, which passes light over the finger or thumb. The same scanner will be installed in the Revaluation machines where the students deposit coins/notes and at the tills where they get their food. A print will be stored numerically, as a set of between 20 and 50 reference points, unique to the individual's print. Each reference point comprises of three numbers which are the X and Y co-ordinates and an angle of curve. The system does not store the image of the finger scanned. The stored co-ordinates are only of use in matching part of the individuals print and cannot be used for the purpose of reconstructing a print. The numbers will be held in a secure SQL database on the server. Access to this database is given only by the school and then only to those who are required to administer the system.

2. The Advantages of Cashless Catering and Biometric Technology: There are several advantages to cashless catering. Students in receipt of free school meals are not identifiable, which can help to avoid a student being stigmatised. In addition, students do not need cash to pay for their lunches that should speed throughout and reduce queues. Biometric technologies can offer some additional advantages over other identification mechanisms:

- Students do not need to remember to bring anything with them to the canteen and there is nothing that can be lost.
- Costs can be reduced as, for example, there is no requirement to replace lost or damaged smartcards.
- It reduces any risk of bullying and theft, as there is no opportunity for students to steal and use other students' smartcards to pay for meals.

3. Registration & Consent

New Year 7 students will be registered for the system during their induction days at KEVICC in July in readiness for starting in September. There will also be an opportunity to discuss and view the system at the Year 6 Parents' Evening.

Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent or carer of a child and obtain the written consent of at least one parent or carer before being able to use a child's biometric information for an automated system.

You should note that the law places specific requirements on Colleges when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

(a) the College *cannot* use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. for use as part of a cashless catering system);

(b) the College must ensure that the information is stored securely;

(c) the College must tell you what it intends to do with the information;

(d) unless the law allows it, the College cannot disclose personal information to another person/body – you should note that the only person/body that the College wishes to share the information with is Biostore, the supplier of the Biometric System, in order to facilitate the continued running and maintenance of the system.

Providing Your Consent/Objecting

As stated above, in order to be able to use your child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the College cannot collect or use his/her biometric information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. His/her objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The contract caterer (Aspens) is also happy to answer any questions you or your child may have. Please contact our Catering Manager, whose contact details are at the end of this information sheet.

If you do not wish your child's biometric information to be processed by the College, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements for children who are not going to use the automated system to access Cashless Catering. The alternative arrangement at the College is the allocation of a computer generated PIN number issued by the catering team. Please note that the College will not accept liability for charges applied to any account caused through misuse or disclosure of PIN numbers, either intentionally or unintentionally by students.

If you give consent to the processing of your child's biometric information, please sign, date and return the section of the admissions form enclosed. Please note that when your child leaves the school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

Further information and guidance

This can be found via the following links:
Department for Education's '*Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff*':
http://www.education.gov.uk/schools/adminandfinance/schooladmin
ICO guide to data protection for organisations:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx
ICO guidance on data protection for education establishments:
http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

4. Information and reassurance about how personal data is used and kept safe:

(Technical Concerns for the use of Biometric Technology at KEVICC)

This document explains the technical nature of the system, and measures in place to address concerns regarding the security of the system. It covers the following:

a. Hardware and Software used
b. Security of Access

a. Hardware and Software used:

The system consists of three main components
a. "Hardware Scanners" which are located at the Tills and Revaluation unit,
b. "SQL Database" which is located on one of the College Secure Servers,
c. "Management Software" which is located on of the College Secure Servers

The hardware scanners take information about the fingerprint of the child. This information is converted to a unique number. An image of the fingerprint is not stored. The data representing each fingerprint is encrypted using the scanner hardware using 256bit AES. The file which is then stored on the system is encrypted again by Secugen using a unique licence for each site. This means that on their own, either piece of information is useless.

Below is an example of a template for a finger.

0X417741414142514141414445415141414151415341414D415A414141414141417477454141 4C714777346C5869656D6C574945494A764A6B42466D6837616C4E764D704F517874517A706A4A395A31784935686C4177395366726E777645576357386C4573314B426F474431666941706755597 04C763168423642682A7043

The solution is secure because the matching can only be done by the individual's consent, since the finger has to be presented to the device for matching. We do not hold an image of fingerprints in our system as the template is stored using the above method. The technology provided for this method of identification meets with BECTA guidelines and also allows students the option to opt out of the scheme and use a PIN number instead. The PIN number is then stored as a replacement for the biometric information.

Furthermore, under the General Data Protection Regulations, the College or caterer (the originator of the data) cannot allow access to this data by anyone for any other means than for the purpose the data was collected. Any biometric data that belongs to an individual that leaves the school is deleted which also meets with the BECTA guidelines.

b. Security of Access

The hardware scanners and individual till points are useless on their own, as no data is stored on these units. All data is stored on the Secure Servers. Although the Servers are located on the College Network, the Cashless Catering system is entirely isolated. There is no dynamic link to SIMS. SIMS data is only used to transfer student details to the system when Students join the College.

Access to the Cashless Catering system is only permitted by our caterers, Network Services staff and Management at the College. This access is fully audited.

Physical access to the machine(s) hosting the system is only permitted by the caterers and Network Services staff. This system and all systems at the College are secured by regularly changing random character passwords. These passwords are only known by Senior Network Services staff. These accounts are time-limited. If the machine(s) hosting the system are removed from the College, the machines will fail to load. If the Hard Drives containing the data for the system are removed from the machines and connected to alternative machines, all held data will be inaccessible as it is encrypted as standard. This is the same for all Secure Servers at the College.

No data is stored on individual computers around the site. All computers on site require valid usernames and passwords in order to provide access – although this access is limited. Administrative access on individual machines is disabled by default – and only enabled by Network Services staff in order to perform maintenance.

Internet Connectivity to the site is provided by the South West Grid for Learning. All inbound access is closely monitored. Individual systems at the College are not accessible unless explicitly requested by Network Services staff. Currently, all access to College systems is via one route – Gateway. This presents a logon screen – which requires College Network usernames and passwords for access. This system audits all activity and, in any case, only allows browsing access to our intranet and associated services. No access is provided to other systems or services.

If you require any further information or wish to discuss how the system works please get in contact and we will be happy to help.

For information on any technical aspects of the system or in respect of the use and handling of data, please contact Ian Wren - Network Manager iwren@kingedwardvi.devon.sch.uk or 01803 869200 ext. 201

To discuss any practical aspects of the daily catering operation, please contact Aspens Services, Catering Manager on catering@kingedwardvi.devon.sch.uk or 01803 869200 ext. 344, or you can call the Catering Department direct on 01803 869228.