



The Warriner School

Introducing Cashless Catering & Parentpay



Dear Parent, Carer or Guardian

Cashless Catering – using biometric data

Harrison Catering our canteen providers run a cashless canteen. Students pay for food using their biometric finger scan. We will aim to undertake Biometric Imaging on your child's first full day at School, or at the earliest and safest opportunity. We are unable to take an image without a signed consent form. It is a legal requirement that we have **your written permission to use this technology**. The Protection of Freedom Act 2012 says:

- *Schools and colleges must notify each parent(s) of a pupil under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system*
- *As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.*

The school requires the written consent of at least one parent/carer to use a pupil's biometric information. **However, consent will be overridden at any time if the other parent/carer objects. If you wish to withdraw your consent at any time, this must be done so in writing to the School.** Also, if a pupil objects to the use of his/her biometric information at any time, the School cannot collect or use that information. If pupils object this can be done verbally at the time or a pupil can withdraw consent at a later date by informing the Finance Department. We would encourage you to discuss your child's right to object or refuse the use of his/her biometric information.

If you are in agreement with your child having a Biometric Image taken please complete the biometric consent form and bring with you along with all other completed forms to your allocated induction session or if you are unable to attend this please return the biometric consent form to the Finance Department.

ParentPay Online Payment System

The school accepts payments online for items such as dinner money, school trips and revision guides etc. using a secure website called ParentPay. ParentPay provides parents with a secure online account, activated using a unique username and password; making a payment using your credit or debit card is straightforward and ParentPay holds an electronic record of all payments for you to view at a later date. When you make a payment, an e-mail confirmation is sent to you, giving you reassurance that the transaction has been successful. Please allow 24hrs for payment to credit your account. Logon details will be forwarded separately. Activation letters should hopefully be available for collection at your allocated induction session.

The implications of becoming a cashless school are that should you send in any payments in cash, you will need to ensure that you send in the correct amount as we are unable to provide change. Payments by cheque, will require a separate cheque of each individual item you wish to pay for.

Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

The Protection of Freedom Act 2012 says:

- *Schools and colleges must notify each parent(s) of a pupil under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system*
- *As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.*

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a code issued to them.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted. As stated above objections must be made to the school in writing.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

The School has appointed Harrison Catering Services Ltd (the "Caterer") to provide a school meals service to its pupils and staff. In pursuance of this legitimate interest the school will share relevant personal data with the Caterer, including pupil name, class and dietary requirements. The Caterer is required to comply with the General Data Protection Regulation in the processing of the personal data.

Frequently Asked Questions

Where is the data stored? In a secure server located within school. This stores the information which identifies pupils uniquely.

How does it work? When you place your finger on the scanner, the software matches your fingerprint with the unique digital signature held in the database

Do you record images of individual fingerprints? No. Fingerprint images are not stored on the system and never will be. Only mathematical representations of certain points of a finger image are recorded, typically between ten and sixty depending on the characteristics of the finger. This mathematical data is encrypted and is called a template. The data is extremely secure in its encrypted form, and even if it were not encrypted it would be impossible to recreate the original fingerprint image from the stored data.

Is it possible to recreate a fingerprint from the data stored? No, the system only stores a short string of encrypted numbers, too little data for the original print to be reconstructed.

How secure is the data stored? The database is protected by a licence key, meaning that the database and any backup of it can only be accessed on licensed hardware. The hardware is stored in the school's own secure facility, so that the encrypted data is only available to the registered licensee. Even if school security was compromised and a backup of data was stolen, the encrypted data would still be unreadable, even by another school.

What happens about twins, or someone who has hurt their finger? Even identical twins have different fingerprints, and will not be mistaken for each other. A cut finger would not cause any problem unless it resulted in major disfigurement.

Could police or a court of law use the fingerprint? The fingerprint image is not stored. The encrypted template is a set of numbers which will be unique within populations of hundreds, or a few thousands of people. However in a wider population it is not accurate enough to be usable for forensic matching with any degree of certainty. A court of law would be unable to use this information as evidence.