Aston Academy

Specialising in Maths & Computing

Executive Principal:
Eunice Newton BEd BA MSc

Associate Principals:
Josie Sanigar BSc (Hons) PGCE, **Rebecca Hibberd** BEd (Hons)

Vice Principal:
Dominic Curran BA(Hons) PGCE

Aughton Road
Swallownest
Sheffield
S26 4SF
Tel: 0114 2872171
Fax: 0114 2876359
E-Mail: info@astonacademy.org
Web: www.astonacademy.org

Dear Parent/Carer

From November 2015, Rotherham Catering Services will be updating our Cashless Catering system at Aston Academy and attached is a leaflet which outlines information about the upgraded system which is based on biometrics.

The system uses an image of the finger, creates a mathematical algorithm and then discards the finger image so that only the numbers remain, which cannot be reinterpreted back into a finger image.

Students, parents, carers and staff can rest assured that the fingerprint images cannot be used by any other source for identification purposes.

In order for your child to use the new system to pay for their meals, you will need to fill out the consent form below. Please sign and return the reply slip below to Reception no later than Monday 21st September.

If you would like to discuss this further then please do not hesitate to contact us.

Yours faithfully

Rebecca Hibberd, Associate Principal

✂--

Please return to Reception by Monday 21st September 2015

Student Name: _____   Reg Group: _____

☐ I **give consent** for my child to use the new biometric cashless catering system.

Signed (Parent/Carer): _____   Date: ___/___/_____

What Are Biometrics?

Biometrics authentication is the automatic recognition of a living being using suitable body characteristics. By measuring an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data, the identity of a specific user is determined. There are many different biometric features that can be used for authentication purposes these include finger image, signature, iris, retina, DNA or any other unique characteristic. Once a characteristic has been chosen the next stage in the Biometric process is authentication. A biometric feature is saved on to a database. Once the data has been stored, a new scanning of the biometric feature is taken. If the comparison is positive, access to the appropriate application is granted.

The history of biometrics

Once the domain of the local constabulary, biometric technology is now being used at many locations around the country. Banks, supermarkets and now even schools and colleges are adopting this increasingly popular technology. Biometrics are not new, their roots have been traced back to ancient Egyptian times. The use of finger images as a security device started with Chinese officials using them to seal documents in the second century BC. Over the last few years the technology has begun to find favour commercially.

Whilst the use of Biometrics has been steadily growing over the last ten years, the past couple of years have seen an explosion in development, interest and vendor involvement.

Biometrics and Security

Students, parents and staff can rest assured that the fingerprint images cannot be used by any other source for identification purposes. The system uses an image of the finger to create a mathematical algorithm and then discards the finger image; only the numbers remain and these cannot be reinterpreted back into a finger image.

The future is in your hands!

Frequently Asked Questions

Why do you need to take my child's finger image?
By taking an image of your child's finger we can turn this information into a digital signature.

Can finger images be used by any other agency?
No, the software we use turns your child's finger image in to a mathematical algorithm. The image of the finger is then discarded. The information that is stored cannot be used to recreate an image of the child's finger.

What happens when my child leaves the School?
When a student leaves school all data can be deleted very easily.

How does it work?
When the child places his/her finger on the scanner, the software matches their finger image with the unique digital signature held in the database.