What is a biometric algorithm?

The individual templates are encrypted using a 256 bit AES key that is built into the scanners hardware. Also the persisted file is encrypted using a different 256 bit AES key built into the matching algorithm supplied by Secugen and generated by a unique license purchased for each site. This is more secure than the ANSII and ISO standards that government department's use as the Secugen Template is encrypted and the ANSII and ISO standards are not. The template data is useless and cannot be interpreted back into a usable fingerprint image. If this was not the case then there would be no world standards and performance measures for such technologies. The data is stored in an array in the RAM of the Biometric Controller and is also permanently stored on the hard drive of the Bio Controller to be restored in the event of a reboot.

Below is an example of a template code for an individual finger.
0X417741414142514141414445415141414151415341414D415A41414141414141417474
774541414C714777346C5869656D6C574945494A764A6B42466D6837616C4E764D7
04F517874517A706A4A395A31784935686C4177395366726E777645576357386C45
73314B426F474431666941706755597 04C763168423642682A7043

The solution is secure because the matching can only be done by the individual's consent as the finger has to be presented to the device for matching. We do not hold images of fingerprints in our system.

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.

Also under the data protection act the school 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 and that is to identify an individual within the solution we supply. Any biometric data that belongs to an individual that leaves the school is purged which also is in line with the BECTA guidelines.

NRS is accredited with ISO27001 – Information Security Management System and is committed to ensuring that privacy is protected. Should we ask you to provide certain information by which you can be identified; you can be assured that it will only be used in accordance with this privacy statement.

The processing of the data is carried out by the School/Catering Company under the General Data Protection Regulation (GDPR) and the Protection of Freedoms Act 2012

Schools' data will remain their responsibility and they remain fully in control of accessing, managing and updating all student data within the system. Schools and the local authority are operating as Data Controllers under the GDPR. All NRS Staff that may have administrator access to schools data for support purposes are Disclosure and Barring Service (DBS) checked.

Information collected to implement a Cashless Catering system is outlined below.

Essential information collected		Optional information may be requested
Admission Number	Gender	Photographs
Surname	Date of Birth	Ethnicity
Forename	Year	School House Group
Form	FSM Allowance	UPN

Nationwide Retail Systems Ltd does not sell, distribute or lease your personal information to third parties.

NRS do not hold any data on premises and all setup and configuration is done on the school/council location.