Calder High School
The Calder Learning Trust
Brier Hey Lane, Mytholmroyd, Hebden Bridge, West Yorkshire HX7 5QN
Tel: 01422 883213 Fax:01422 881876
Email: admin@calderlearningtrust.com / parentenquiry@calderlearningtrust.com
Web: www.calderlearningtrust.com
Headteacher: Mr A Guise

CONSENT FORM FOR THE USE OF BIOMETRIC (FINGERPRINT)

Please complete this form if you consent to the school (The Calder Learning Trust) taking your child's fingerprint as part the schools cashless catering system. This biometric information will be used by the school for the purpose of identifying at point of sale in the canteen and food pre-order points and at no point will this data be taken off or from the internal systems within school.

In signing this form, you are authorising the school to use your child's biometric information for this purpose until he/she either leaves the school or ceases to use the system. If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school.

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school.

Having read guidance provided to me by the school, I give consent to information from the fingerprint of my son/daughter being taken and used by the school for use as part of the cashless catering system.

I understand that I can withdraw this consent at any time in writing.

Name of Parent: ……..

Name of Student: …… **Form:** ……

Signature: ……

Date: ……

INFORMATION ON FINGERPRINTS (BIOMETRICS):-

The individual fingerprints 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.

0X417741414142514141414445415141414151415341414D415A41414141414141747
74541414C714777346C5869656D6C574945494A764A6B42466D6837616C4E764D70
4F517874517A706A4A395A31784935686C4177395366726E777645576357386C4573
314B426F474431666941706755597 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.