



BIOMETRICS POLICY

2009-2010

Lead Person: Assistant Head
Governing Body Committee: Asset Management

INTRODUCTION

The reason for this policy is to enable the use of library software that uses fingerprint scanning to speed up book issue and to give students greater security over their user identity. A policy is required because of the data protection issues raised by fingerprint scanning.

The school library database (Heritage Online) stores detailed information about all of the books, CDs, DVDs and videos held in the library. It has the capacity to act as an inventory for the whole school, listing where portable items are kept on site and being able to check them out and back in, issuing reminders and fines when and if appropriate.

Heritage Online also has a database of the names of all students and staff, their Reader Number and PIN, their dates of birth, a history of the items they have borrowed and the content they have searched for. The dates of birth are stored to identify year group and to restrict circulation of some items to specific age ranges. The 4 digit PIN is randomly generated, can be altered, and acts as the students' password when they log-in to their Heritage account online to reserve books online or to add electronic book reviews.

Any personal data that is stored falls under the Data Protection Act. The personal data stored in the Heritage database are names and dates of birth.

Heritage has a module that allows items to be issued by scanning the book and identifying a fingerprint of the student or member of staff borrowing the item (hereafter given as the Reader). Fingerprints are not essential to the application but, unlike library cards, they cannot be lost or left at home.

As personal biometric data (i.e. fingerprints) are sensitive personal data, it is important to have a record of the facts about the system and a policy on its use.

FACTUAL BACKGROUND

The data protection issues surrounding the safeguarding of "high level" biometric data (e.g. fingerprint images) would be significant. The Crypt School would not want to have a system that requires high levels of data protection.

The Heritage system does not store fingerprint images. The scanner sees the fingerprint and “samples” points of what it sees. Based on the pattern of lines and junctions in the samples, the scanner makes a number and sends that to the computer. So the scanner sees fingerprints and uses them to make Reader Numbers. What the computer receives is a library card number, not a fingerprint. It may be hypothetically possible to make a machine that “reverse engineers” the library card number to re-create the sample points. What would be made would be a schematic representation of patches of a fingerprint, not a full or a detailed fingerprint. No such machine exists.

If it were possible to create a machine that generated a full fingerprint, the risk would be low-likelihood but high-consequence. As it is not even hypothetically possible to generate a full fingerprint, this is a low-likelihood and low-consequence situation.

For the purposes of the Data Protection Act, the Readers (students or staff) are the “data subjects”. It is they who must be informed and consulted about the use of their personal data. There is nothing in the Act that states that until a child has reached a specific age any data protection rights they have should be exercised by their parents/guardians. Furthermore, there is nothing in the Act that requires schools to seek consent from parents/guardians before implementing a fingerprint-based application. However, it is clearly desirable that parents/guardians should be fully informed and that students should discuss the matter with adults before being asked for biometric data. As a school, we would wish students to be conscious of their civil liberties and to make rational and informed decisions about the level of risk when giving biometric data to any agency during their lives.

THE CRYPT SCHOOL – POLICY ON BIOMETRICS

This policy has been prepared with reference to the Information Commissioner’s Office report on Biometrics in Schools V1.1 August 2008. All named persons are current as of October 2009.

All students and staff joining the school are to be issued with information about the nature of the fingerprint-based system and what personal data is stored by the system.

- Responsible for providing and updating the information: line manager for the Library – Head of English
- Responsible for informing new students: Office Manager
- Responsible for informing new staff: Assistant Head i/c new staff induction

Regardless of the risk, some students, students’ parents or staff may simply feel uncomfortable about giving fingerprint-based data. In this event, a student or member of staff has the option not to use a fingerprint to create and scan their Reader Number. In the case of a student, this must then be followed up by a letter from a parent or guardian requesting a library card with a barcode. The librarian will keep a stock of standard letters for students to take home in this event.

- Responsible for logging student data: Librarian
- Responsible for issuing letter informing parents/guardians of choice not to use fingerprints: Librarian
- Responsible for issue of library cards on receipt of written request: Librarian

All personal data should only be kept in school for as long as it fulfils its specific purpose. There is no reason to retain the names and dates of birth of students or staff within the Heritage system after they have left the school. The Reader record must be deleted as soon as is practical after the Reader leaves the school, normally at the start of a new academic year.

- Responsible for informing Librarian of non-Y13 leavers: Data Manager
- Responsible for deleting Reader records: Librarian

The personal data stored (names and dates of birth) must be protected from unauthorised access. This information can only be accessed from the Administrator account, which will only allow one user on one machine at any given time. As with all access to personal data, the username and password for this account should be restricted on a need-to-know basis. Currently, those with a need to know are the Head IT Technician, the Librarian and the line manager for the library (Head of English).

Annexes:

A – The Data Protection Principles

B – Letter to new students and staff, informing them of the purpose of scanning their fingerprints

C – Letter to parents/guardians informing them of the purpose of scanning students' fingerprints

Annexe A:

The Data Protection Act 1998 includes eight data protection principles with which data controllers must comply. The first, second, fifth and seventh principles are the most relevant to this issue.

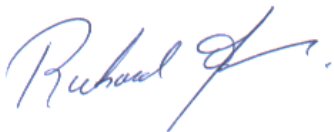
The first principle requires that personal data is processed fairly and lawfully. Fairness requires that schools ensure that pupils are informed about and understand the purpose for which their personal data is being processed.

The second principle requires that personal data is obtained for one or more specified and lawful purposes and not further processed in any manner incompatible with that purpose or those purposes. Children's biometric data should therefore not be used for any purpose not directly related to that for which it was collected.

The fifth principle requires that personal data is not kept for longer than it is needed for its specified purpose. Pupils' biometric data should therefore be destroyed when they have left the school.

The seventh principle requires that the appropriate security is in place to safeguard personal data from unauthorised processing and accidental loss, destruction or damage.

Annexes B and C to be written
Approved :



Chair of Governors

Review : December 2010