CRB Cunninghams GDPR Summary Statement - March 2018

The ICO have published guides for educational establishments GDPR Advice.

To help schools comply with GPDR we are providing the following information and advice.

OUR ROLE

We act as a data processor when we remotely connect to the school to assist with maintenance routines, imports etc.

As an organisation we are accredited with **ISO/IEC 27001** certification, we have audited our current policies, procedures and software to ensure that they meet the requirements of the GDPR.

SCOPE

CRB Cunninghams software products hold Personal Data sourced from the school MIS (or created manually), the data is used to verify the identity of an individual at the point of service delivery via computer terminals, EPOS terminals, Coin & Note revaluation units, self-service kiosks, registration terminals, printers, lockers and other similar devices within the customers premises and subsequently allow them to use the services provided by that software product.

The categories of data subject to whom the Personal Data relates

Pupils, Students, Employees and any authorised visitors that require access to related services.

The types of Personal Data to be processed

Commonly Held data includes: - Surname, Legal Surname, Forename, Registration Group, Year, Date of Birth, Gender, Free Meal Eligibility, Admission Number, MISID, Photograph, Biometric template*****

Optionally held data includes: - Tutor, Address, Postcode, Telephone, Email, Dietary preferences, Parental Consent, UPN, Dietary needs*****

Transactional data

Purchases, credits, refunds, attendance data. These are related to personal records using a system generated identifier.

Biometric Data *

Biometric data (fingerprints) are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored. The

encryption standard used for encrypting the data points is AES 256 with the symmetric key being stored in RSA 2048 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf The AES 256 encryption standard is used for storing top secret designated data by the American military and the NSA. Both AES and RSA are well used and commonly understood encryption standards that cannot be broken by brute force in a reasonable time.

***** These are defined as "sensitive data"

SECURITY

How do CRB Cunninghams products ensure that personal data is securely held?

Access to data is controlled by user/group permissions. These can be configured to allow/deny users access to view/edit individual fields and reports. It is the data controller's responsibility to determine what access individual users should be allowed.

The data controller must ensure that the software database tables are held securely within the school. This includes ensuring the server on which it is being stored should have up to date anti-virus software, it should be in a physically secure location and folder permissions should be restricted to authorised users.

ENCRYPTION

Historically only user logins and passwords plus biometric data were encrypted. GDPR does not require but does recommend that personal and sensitive data should be encrypted. This enhanced non-regulatory feature has now been added to our software and will be rolled out to existing sites in due course as scheduled upgrades.

DATA RETENTION

It is the data controller's responsibility to ensure that data is not retained for "longer than necessary". Our software data is typically archived on an annual basis. This data is available to be reported on until the school decides it is no longer required.

DATA SHARING

If schools use third party internet payments interfaced to our software, then relevant data will be shared with the payment provider. While CRB Cunninghams are talking to the providers to ensure they are compliant the decision to share data is the responsibility of the data controller.

DATA ACCESS

GDPR gives the right to individuals to access their personal data and supplementary information held about them. Currently this information is not held in a single report. CRB Cunninghams intend to make a tool available which allows all data to be supplied in a single report to help satisfy these requests should they arise. This tool will be issued as a scheduled upgrade but can be made available on request.