Privacy Impact Assessment

CASHLESS CATERING

Privacy Impact Assessment – Screening Questions

Question	Y/N	Additional Comments (please give reasons for either a 'yes' or' no 'answer here)
Is there a requirement under GDPR to carry out a PIA? NB if there is a legal requirement to carry out a PIA there is no requirement to complete the remaining questions.	N	
Will the project involve the collection of new information about individuals?	N	All personal data is securely held within School/DCC systems. Existing scope of information collected about individuals will not change.
Will the project compel individuals to provide information about themselves?	N	
Will information about individuals be disclosed to third party organisations or people?	N	Pupil data is securely held within School/DCC system therefore no requirement to disclose to the third party administrating the system. There is no requirement to disclose information concerning individuals to third party organisations or people when operating the system.
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	No alteration to the scope or purpose concerning the usage of the information.
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	Y	Possible use of fingerprint recognition to replace card swipes in order to access their accounts. Card method still available if preferred.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	N	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, health or information concerning an individual's sex life or sexual orientation or other information that people would consider to be private.	N	None of the data held about individuals is likely to raise privacy concerns. The potential use of biometric data (fingerprints) is purely held to identify a specific individual's information on the system, photographs are also used but this again is to aid in the security of the cashless catering account not being used by another pupil.
Will the project require you to contact individuals in ways that they may find intrusive?	N	
Will the data be held in relation to children or vulnerable adults?	N	All personal data is securely held within School/DCC systems. The retained information relates to non-vulnerable children.

Privacy Impact Assessment

Step 1 – Requirement for PIA – issues to be addressed

To Include:

- Project Aim and Objectives

To provide a cashless environment in secondary schools across Derbyshire for the purchasing of school meals and refreshments. To improve efficiencies by reducing over catering, and therefore help reduce food wasted in schools.

- Benefits to the organisation, to individuals and to other parties of personal data

The cashless catering facility allows students to purchase food and drink via fingerprint recognition technology which identifies the student and opens their catering account. A swipe card system is also in use for students whose parents have opted for them not to use fingerprint recognition and for visitors. The student's catering account can be topped up by cash, cheque or online.
The system holds the student's name, class, photograph (to prevent a lost or stolen card being used by someone else), account balance and meal entitlement.

The benefits for catering staff are that they do not have to handle cash and the system produces all of their financial and stock reports.
The benefits for students are less time queuing for meals, a reduced need to carry money with them, foods with ingredients that cause allergic reactions can be automatically blocked for them, and the 'stigma' of free school meals is removed as the system automatically credits eligible students' accounts each day.
Furthermore, parents can set a daily spend limit and obtain a report of their child's transactions including the items purchased.

- Links to any relevant project documentation

Cashless Catering Business case - N:\PROJECTS\1 Active Projects\4 Systems Procurement and Implementation\14 Cashless Catering\Business Case for Cashless Catering System in Schools.docx

- Summary of Identified Need for PIA (can draw on answers to the screening questions).

Due to the possible use of fingerprint recognition to replace card swipes in order to access accounts, this biometric data has identified the need for a full PIA.

Step 2 – Information Flows/Nature of processing

To Include:

- Description of collection, use, retention and deletion of personal data- is any sharing of data involved?

Response from CRB Cunninghams - Online payment portals and implements and maintains encrypted integration
It is the policy of CRB Cunningham's to comply with the terms of the Data protection Act 1998 and any subsequent legislation to achieve high standards in the handling of personal information
CRB Cunningham's can ensure full compliance with the General Data Protection Regulations to ensure the protection of the rights of data subjects.
Our solutions are compliant with all relevant standards, laws and regulations surrounding data security, GDPR, cyber security and PCI compliance, we are ISO27001 certified. We have provided evidence by way of our GDPR compliance statement & ISO27001 certificate attached and sent when submitting the tender

Response from Nationwide - The system we will be using is on the school's infrastructure and the data processing is carried out by automated means either through the MIS extractor or by employees of the school/outsourced catering personnel who operate the Trust-e Cashless Catering System.
Although we are not the Data Processor we do acknowledge that all schools require our support in understanding what data is processed.

- Explanation of data flows – diagram or description detailing: controllers and processors, storage location and storage method, personal data fields collected, individual/team/organisational access to personal data(audit trail), security measures for storage and transfer of data

Response from 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 site and allow them to use the services provided by that software.
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.

- Number of individuals likely to be affected by the project-do they include children or other vulnerable groups?

Cashless catering is aimed at Secondary School age pupils and covers 21 Secondary Schools in Derbyshire (circa 18,000 pupils).

- A flow diagram is likely to be helpful here.

CRB Cunninghams - http://crbcunninghams.co.uk/download/cashless-system-technical-overview/

- Does the data include special category or criminal offence data?

Biometric data in the form of a fingerprint can be stored on the account and linked to other data about the student.

Step 2 – Consultation Requirements

Identify whether internal and/or external consultation is required to address privacy risks

- Stakeholders to be consulted

Secondary Schools, pupils, parents, DCC Catering Services, Children's Services Information and ICT, Corporate Projects

- Method of consultation

Derbyshire County Council have been working closely with all Secondary Schools in the implementation of this system directly with secondary schools. Newsletters have been developed and issues to parents. Ongoing consultation will be taking place between DCC's Catering Service and Schools.

Part B Steps 3 to 4 – Identify Privacy Risks, Solutions and Approval

Privacy Risk	Risk to Individuals & organisation	Risk initial score	Action Identified	Target Score (after applying actions)	Risk Control Plan (Treat/ Control/ Tolerate/ Accept/ Terminate/ Transfer)	Evaluation: is the final impact on individuals and the organisation after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Approved By
System data (including biometric data) is accessed by unauthorised persons and used or shared inappropriately	Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information. Financial and reputational damage. Legal action could be taken against the LA and possible substantial fine.	8	Access to the system will be limited to only those with the correct role based access activity. Software used to process biometric data turns the fingerprint into a mathematical algorithm. This information cannot be used to recreate the fingerprint. As part of the tendering process all suppliers of cashless catering have correct policies and procedures in place to minimise this risk. All suppliers have agreed to adhere to DCC's Supplier Information Security Policy, Information Backup and Restore Policy and Data Protection and Storage Media Handling Procedures	4			

Data is not maintained to ensure information held is relevant, up to date and accurate	Breach of data protection act. Financial and reputational damage.	8	Determine validation checks on the data stored meets data protection requirements and information retention responsibilities. Review accuracy of data stored. Ensure correct processes are followed in accordance with DCC policy	4			
Data is lost/stolen and thus unable to be accessed by system	Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information. Financial and reputational damage. Legal action could be taken against the LA and possible substantial fine. Inability of individual(s) to use systems and access service.	8	As per above.	4			

Step four: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Update CS retention schedule (Where necessary)	31st Aug 2018	
Update CS Information Audit (Where necessary)	31st Aug 2018	

Contact point for future privacy concerns
Date of consideration by IGG: 6th August 2018

Linking the PIA to the GDPR principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

- Have you identified the purpose of the project and which lawful basis applies? (B)
- Is the processing of the data necessary in terms of GDPR? Yes
- How will you tell individuals about the use of their personal data?

When Schools set up cashless catering accounts with parents they will issue appropriate guidance.

- Do you need to amend your privacy notices? No
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? N/A
- If special categories of personal data have been identified have the requirements of GDPR been met? Yes

As the Council is subject to the Human Rights Act, you will also need to consider where privacy risk are especially high need to consider:

- Will your actions interfere with the right to privacy under Article 8? No
- Have you identified the social need and aims of the project? Yes
- Are your actions a proportionate response to the social need? Yes

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data? Yes
- Have you identified potential new purposes as the scope of the project expands? No
- Does your Privacy Notice cover all potential users? N/A

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the quality of the information good enough for the purposes it is used? Yes
- Which personal data could you not use, without compromising the needs of the project?

None – based on the security of the cashless catering system

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary? Yes
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Using verified data from Schools MI

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

- What retention periods are suitable for the personal data you will be processing?

7 years – financial data

- Are you procuring software that will allow you to delete information in line with your retention periods? **Yes**

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under GDPR.

- Will the systems you are putting in place allow you to respond to subject access requests more easily? **Yes**
- Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten). **Yes**
- If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose? **N/A**

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified? **Yes**
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

On-site training is provided by the schools for the catering staff and technical support is available as part of the contract

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA? **No**
- If you will be making transfers, how will you ensure that the data is adequately protected? **N/A**