DERBYSHIRE
County Council

Information Security Document

Early Years and Education Management Information System Privacy Impact Assessment

Version 0.1

Version History			
Version	**Date**	**Detail**	**Author**
0.1	20/11/17	First Draft	
0.2	16/01/18	Second Draft	
0.3		Final Review and approval at IGG	
0.3		Review by IGG	
0.4		Further amendments	

CONTENTS

Contents	Page
Section 1 - Privacy Impact Assessment Screening Questions	4
Section 2 - Privacy Impact Assessment:	
- Step one: Identify the need for a PIA	5
- Step two: Describe the information flows	7
- Consultation requirements	9
- Step three: Identify the privacy and related risk	10
- Step four: Identify privacy solutions	12
- Step five: Sign off and record the PIA outcomes	14
- Step six: Integrate the PIA outcomes back into the project plan	14
Section 3 - Linking the PIA to the Data Protection Principles	15

Section 1 - Privacy Impact Assessment Screening Questions

Will the project involve the collection of new information about individuals?	YES
Will the project compel individuals to provide information about themselves?	YES
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	NO
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	NO
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.	NO
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	YES
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	YES
Will the project require you to contact individuals in ways that they may find intrusive?	NO

Section 2 - Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal.
Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The existing contract for the Early Years and Education Management Information System (EYE-MIS) is due to expire in 2019. As a result, the Council is embarking on a re-procurement project. The existing IT system is a business critical system used within Children's Services to support the delivery of a number of statutory functions. The Children's Services work areas covered by this re-procurement project include:

- SEND (Special Educational Needs and Disabilities)
- Inclusion
- Elective Home Education
- Education Welfare
- IPT and Out of School Tuition
- Behaviour Support
- Education Psychology
- Autism Outreach and Sensory and Physical Support
- Virtual School
- School Admissions and Transport
- Family Information Services
- Childcare Sufficiency
- Catering including Free School Meals
- Early Years Finance
- Governor Support
- Integrated Workforce Development Team

As well as re-procuring functionality that is already utilised, Children's Services are keen to explore new modules and enhancements, including interfacing with the Social Care Case Management System – Mosaic, to enhance and streamline existing work processes across the numerous Children's Services work areas.

Other aims and benefits include:

- To provide a fit for purpose system to support statutory and non-statutory services across the Education and Early Years functions within Children's Services.
- Improved decision making by bringing information together, complete with history and family context.
- Improved visibility of other agencies working with a child or family.
- Improved service delivery standards.
- Comprehensive data security management by ensuring that information is shared in a targeted way, by only making information available to those practitioners who really need it.
- Improved data integrity and accuracy.
- Flexible and robust reporting and analysis.
- Enhanced safeguarding and protection of vulnerable children, by ensuring that all the information known about a child or family is available in one place, and to appropriate professionals.
- Flexible and mobile working from any location.
- Sharing of information with other agencies/voluntary sector and partners, schools and other local authorities.
- Improved visibility of other agencies working with a child or family.
- Auditing of activity to ensure that any breach or misuse can be fully tracked.
- The provision of a flexible platform that can be reconfigured and easily changed to reflect changes in legislation, service practice or organisational restructures.
- Use of the system(s) by all staff, partners, agencies and the public in a flexible and configurable manner, within and ideally beyond Derbyshire's administrative borders.

The need for a PIA has been identified due to the personal information that is required to be collected and stored, of both children and their families. The information will be provided by schools, parents/guardians and ….

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

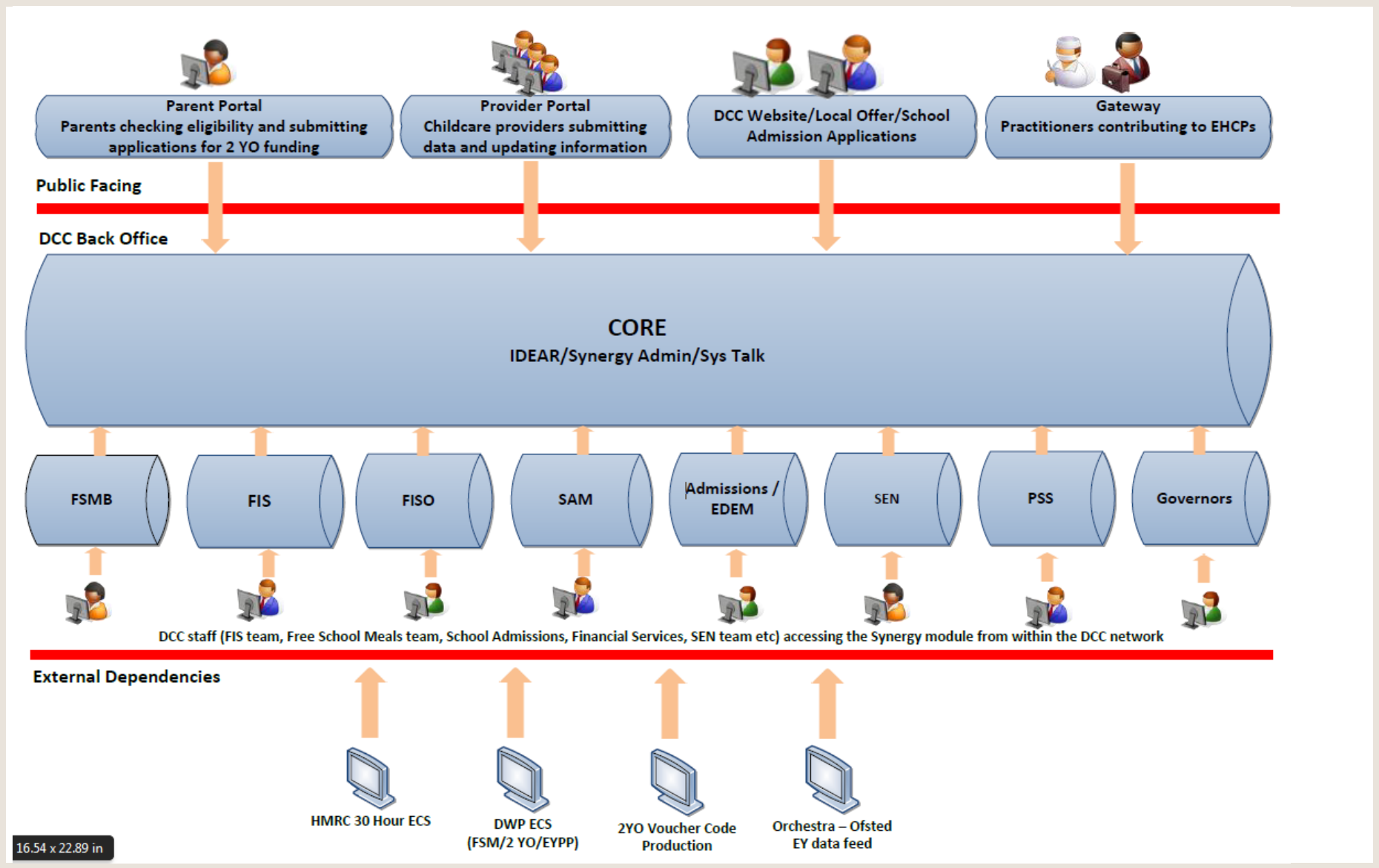
The collection of personal data is obtained from a variety of sources including portals (where the data is automatically updated into the EYE-MIS), schools IT systems, paper forms and telephone referrals. The data collected is both confidential and personal in nature; examples include names, addresses, date of birth and NHS number, as well as schools attended, and any pupil support including, for example, free school meals, schools transport and pupil support services.

The data is accessed via different modules, dependent upon the work area, and is controlled by assigning role-based access permissions to the system users. Some work areas overlap and there is therefore a requirement for some of these to have access to more than one module. It is the responsibility of Children's Services to determine who should have appropriate role based access to view or amend the data.

The system receives regular feeds from School Management Information Systems to update and maintain pupil details, and is also accessed by parents and carers through on-line applications processed (eg. Admissions, Early Years Free Child Care, etc), along with the potential for Health and Social Care practitioners to support the development of Education, Health and Care Plans.

Data from the system is used to source the requirements of a number of Central Government Statutory Returns and the regulatory inspection frameworks of Ofsted.

The diagram below illustrates the flow of information between the external systems and the existing EYE-MIS system.


Parent Portal
Parents checking eligibility and submitting applications for 2 YO funding
Provider Portal
Childcare providers submitting data and updating information
DCC Website/Local Offer/School Admission Applications
Gateway
Practitioners contributing to EHCPs
Public Facing
DCC Back Office
CORE
IDEAR/Synergy Admin/Sys Talk
FSMB
FIS
FISO
SAM
Admissions / EDEM
SEN
PSS
Governors
DCC staff (FIS team, Free School Meals team, School Admissions, Financial Services, SEN team etc) accessing the Synergy module from within the DCC network
External Dependencies
HMRC 30 Hour ECS
DWP ECS (FSM/2 YO/EYPP)
2YO Voucher Code Production
Orchestra – Ofsted EY data feed
16.54 x 22.89 in

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

A project board has been established, which is led by an Assistant Director in Children's Services. The project board will be responsible for a number of aims and objectives, including dealing with any risks/issues, ensuring that there is a cohesive approach in meeting the overall aims of the project and setting and monitoring the delivery of the identified priorities. This board will also own the PIA and risks/mitigations identified.

A business case for the re-procurement of the system has been produced and agreed by Children's Services SMT. The business case is an evolving document and will be adapted and changed as required. These changes will be signed off by the project board before being sent for approval by Children's Services SMT.

Consultation will continue to be undertaken with all Children's Services work areas that use the existing system. A stakeholder and communications document has been produced which identifies managers and users of each work area and the methods of communication to be used throughout the project.

The development of the most recent Information Sharing Agreements with schools has been completed in consultation with them. This included the purpose for sharing, consent and secure extraction of information from their system to update the central pupil database.

Communications with parents and carers on the recent SEND reforms and 30 hour free child care offer has been completed in order to consult on the legislative changes and to gain feedback on the Council's approach.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
Section 3 can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
System 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	Breach of Principle 7 of the Data Protection Act	Financial and reputational damage. Legal action could be taken against the LA and possible substantial fine
If a retention period is not established Information might be used for longer than necessary.	Data becomes out of date and could be inaccurate	Breach of Data Protection Principles 4 and 5	Financial and reputational damage
Data collection, storage and processing creates a risk of confidential information being accessed without the	Individuals' privacy is compromised and data is shared beyond the organisation they expect.	Reliance on all organisations to comply with data sharing agreements.	Reputational damage

knowledge or consent of the child/young person. Ensuring data subjects, i.e. a child/younger person, are aware of rights under data protection legislation relating to processing of data for these requirements.	Individual's privacy is compromised by breaching rights of a data subject in relation to their personal data, including right to withdraw consent.	Breach of Principle 6 of the Data Protection Act	Reputational damage and potential fines

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
System data is accessed by unauthorised persons and used or shared inappropriately.	Access to the system will be limited to only those with the correct role based access activity. The use of the system will be managed locally through relevant training and guidance to practitioners. Limited information will be shared, and any that is shared will be covered by data sharing agreements.	Accepted/Reduced	
If a retention period is not established Information might be used for longer than necessary.	The information about a child will be stored within the system/archive in accordance with the Council's Records Retention Schedule. Any data that has met the retention expiry date will be deleted.	Eliminated	

Data collection, storage and processing creates a risk of confidential information being accessed without the knowledge or consent of the child/young person.	The Children's Act 1989, 2004 and Human Rights Act 1998, in addition to other policy drivers have been consulted to ensure that consent to share any child information would not breach any confidentiality or privacy issues, where it is deemed necessary to share the information.	Eliminated	
To ensure data subjects are aware of their rights regarding their personal data, including their right to withdraw consent at any time and the process for doing so. Ensuring data subjects, i.e. a child/younger person, are aware of rights under data protection legislation relating to processing of data for these requirements.	All consent forms used to collect personal data used by the Local Authority will be compliant with the new GDPR regulations and will refer to rights of data subjects, including right to withdraw consent and process for doing so. All Local Authority Privacy Notices will be updated to reflect any system changes and ensure they cover the rights of data subjects in relation to the personal information it holds about them.	Accepted/Reduced	

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As outlined in step 4	As outlined in step 4	

Step six: 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
Project Governance and controls including highlight reports to be completed during the life span of the project.	Ongoing	
Testing of technical solutions and controls before 'Go-Live'.	TBC	
Oversight and evaluation of the project against the success criteria.	TBC	
Contact point for future privacy concerns		

Section 3 - Linking the PIA to the Data Protection 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 DPA or other relevant legislation, for example the Human Rights Act.

Principle 1 - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: **a) at least one of the conditions in Schedule 2 is met, and** **b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**	
Have you identified the purpose of the project?	Yes
How will you tell individuals about the use of their personal data?	Privacy Notices and consent forms
Do you need to amend your privacy notices?	No
Have you established which conditions for processing apply?	Yes
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?	Soft Market Testing will inform
If your organisation is subject to the Human Rights Act, you also 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 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?	Soft Market Testing will inform

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?	N/A

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?	Use of other systems to validate data – eg, School MI systems, Social Care Case Management System etc

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	
What retention periods are suitable for the personal data you will be processing?	See Records Retention Schedule
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 this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	Yes
If the project involves marketing, have you got a procedure for individuals to opt out of 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?	Training for all users for the new system, delivered by the supplier, and ongoing training for new starters via e-learning.

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