PRIVACY IMPACT ASSESSMENT - Advanced

The assessment should be completed at the **planning stage** to ensure that risks are identified early and managed effectively **before** the project/work is started. Identified risks should be included the project risk assessment/register and any changes to the project plan should be reflected in the privacy impact assessment. The IG Checklist (Privacy Impact Assessment) is a risk management process that enables any participating organisation to anticipate and address likely impacts of new initiatives, to provide assurance of confidentiality, data protection, IT security and data quality issues related to this project. This completed assessment should be referenced and embedded in the Business Case Approval papers.

Privacy impact assessments are mandatory for any new system (IT or otherwise), process or technology which involves person identifiable or business sensitive data. **Completed assessments must be sent to the Information and Records Team. (data.protection@cambridgeshire.gov.uk)**

Title	**Mosaic**
Project Outline	Mosaic is the new system, supplied by Servelec HSC, to support Adults Early Help and Social Care, and Children's Early Help and Social Care. For Adult Social Care, Mosaic will replace SWIFT AIS and Adult Finance Module (AFM). For Children's Social Care, it will replace case management elements of Capita One.
Organisations Involved (a complete list of all of the stakeholders including those departments or organisations that have an interest in, a role to play in the delivery, or may be affected by the project)	Cambridgeshire County Council • Chief Executive • Corporate and Customer Services • People and Communities • Resources • Shared Services - LGSS People and Communities • Adults and Safeguarding • Children's and Safeguarding • Older People and Mental Health • Education • Commissioning

	Corporate and Customer Services • Customer Services • Business Intelligence • Corporate Information Management • Communications and Information • IT & Digital Services • Business Continuity • Information Governance Team Place and Economy Resources • Transformation LGSS • IT (inc. IS Training Team) • Finance (inc. Enterprise Resource Planning (ERP Gold/Agresso Project) • HR Health • CPFT (Mental Health) • CPFT (Health staff within the Learning Disability Partnership) • CCG Suppliers • Servelec HSC • Northgate • Capita One Others • Members

	• Public Health • Health • VCS • Multi Agency Referral Unit (MARU)
Data and information Provide a list of the datasets/types of Person Identifiable Data (PID) involved. 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.	**Cambridgeshire County Council like all organisations that process and store identifiable data, must protect the confidentiality of that data and must guard against risks and threats from inside and outside the organisation.** Information concerning the data extract can be found in **Appendix 1a Data Extract**. **Statutory Returns** **Service areas – Early Help etc.**
Data Protection	

Data Controllers and Data Processor Name the data controller and list all organisations that will be processing data on behalf of the data controller. Provide details of the individual who will be considered to be the Information Asset Owner. Is there a process for managing incidents relating to information breaches/losses and reporting those to the data controller?	**Data Controllers** **SIRO –Sue Grace** **Caldecott guardian – Claire Bruin** **Information Asset Owners - Directors of ASC/ CS** Charlotte Black – Adults and Safeguarding Lou Williams – Children's and Safeguarding **All organisations that will be processing data on behalf of the data controller.** Cambridgeshire County Council • Chief Executive • Corporate and Customer Services • People and Communities • Resources • Shared Services - LGSS People and Communities • Adults and Safeguarding • Children's and Safeguarding • Older People and Mental Health • Education • Commissioning Resources • Transformation Place and Economy LGSS • IT (inc. IS Training Team) • Finance (inc. Enterprise Resource Planning (ERP Gold/Agresso Project)

	• HR Health • CPFT (Mental Health) • CPFT (Health staff within the Learning Disability Partnership) • CCG Suppliers • Servelec HSC • Northgate • Capita One Others • Members • Public Health • Health • VCS • Multi Agency Referral Unit (MARU) • Service Providers/Suppliers **Information Management Policy Framework** is the process for managing incidents relating to information breaches/losses and reporting those to the data controller.
Systems – what IT systems are involved?	**As at Sept 2017 –** Mosaic, Wisdom, Agresso, NHS Mini Spine, Address Gazetteer. **Future systems** (to be confirmed) – Capita One, MS Dynamics, Aspire, Cygnum **Reporting tools** (to be confirmed) - Business Objects, SSRS, Corius **'To be' archiving system** (data warehouse)

	Target systems - Department for Education Collect system (SSDA 903 return, CIN Census, fostering return, adoption returns) NCCIS, Department of Health data returns, SALT return, SAC return, User experience surveys, National Fraud Initiative
Datasets Provide a list of the datasets/types of Person Identifiable Data (PID) involved.	Name, address, postcode, date of birth and NHS number, Unique pupil number, national insurance number, Legacy Person Reference, Legacy System id.
Provide a list of all types of sensitive data that will be collected. (i.e. ethnicity, religious beliefs etc.)	Gender, Ethnicity, First Language, Religion, Nationality, Country of Birth, Marital Status, Conditions and disability, Illnesses, Strength and Difficulty scores, Health Checks, Immunisations, Criminal offences**.**
Is personal data / sensitive personal data being processed? If so, how? How will you communicate to those involve that their personal data is being processed?	Personal **and** sensitive personal data will be processed in Mosaic for both Adults and Children's service users. Communication to those involved that their personal data is being processed will be through the use of Privacy Notices, reinforcing current local practice, Form design, Privacy Notice, Information Security Training, Data Protection Training.
List the purpose(s) for handling/collecting person identifiable data?	**Person identifiable data is necessary for safeguarding, intervention and specific programmes of research in Adults and Children's services -** Access and Short Term Management Adult Customer Services Adult Early Help Adult MASH Adult Social Care

	Adults Customer Care Team Adults EDT Technology Enabled Care Brokerage Care Network Carers Trust Cambridgeshire Peterborough Norfolk Counting Every Adult Complex and Long Term Management Continuing Health Care Team Contracts CPFT Community OT CPFT Mental Health Direct Payment Monitoring Discharge North Discharge Planning Management Discharge South DoLS Double Up Team Enhanced Response Service LDP City and South Cambridgeshire LDP East Cambridgeshire LDP Fenland LDP Huntingdon LDP Management LDP North Service Area LDP South Service Area LGSS Appointee & Deputyship LGSS Financial Assessment Team Neighbourhood Cares Older People Services OP City and South Cambridgeshire OP East Cambridgeshire OP Fenland

	OP Huntingdon Physical Disabilities Team Practice and Safeguarding (Adults) Quality Governance and Practice Development Team Reablement Management Reablement North Reablement South Sensory Service Young Carers Service 14 - 25 Additional Needs Team Camb City Unit 1 Camb City Unit 2 Camb City Unit 3 Camb City Unit 4 Camb City Unit 5 Camb City Unit 6 CCA CEP Business Support Children and Safeguarding Child and Family Centre Wisbech Child and Family Centre Huntingdonshire Child and Family Centre East Cambs Child and Family Centre South Cambs Child and Family Centre Cambridge City Child and Family Centre Huntingdon Town Child and Family Centre Ormiston Child and Family Centres Children's Customer Care Team Children's Customer Services Children's EDT Children's Participation Team Children's Services Clinical Team

	Commissioning Community Support Service Duty Team Countywide and LAC CREDS Disability Unit North Disability Unit South Disabled Children's Early Help Team Disabled Children's Social Care Team North Disabled Children's Social Care Team South Drugs and Alcohol and Domestic Violence Early Help Cambridge City Early Help East Cambridgeshire Early Help Hub Early Help Huntingdon and St Ives Early Help Management Early Help March, Chatteris and Whittlesey Early Help North Early Help South Early Help South Cambridgeshire Early Help St Neots and RSY Early Help Wisbech East Cambs Unit 1 East Cambs Unit 2 East Cambs Unit 3 East Cambs Unit 4 East Cambs Unit 5 Education Child Protection Service First Response Central First Response North First Response South Fostering Fostering Assessment Fostering Duty and Family Finding

	Fostering Link Fostering Support Housing Communities and Youth Hunts Unit 1 Hunts Unit 2 Hunts Unit 3 Hunts Unit 4 Hunts Unit 5 Hunts Unit 6 Hunts Unit 7 Hunts Unit 8 Hunts Unit 9 Integrated Front Door LAC (14-25) Team 1 LAC (14-25) Team 2 LAC (14-25) Team 3 LAC (14-25) Team 4 LAC IRO Service LADO LDP Young Adults Team Learning Directorate LSCB March, Chatteris and Whittlesey Unit 5 March, Chatteris and Whittlesey Unit 6 March, Chatteris and Whittlesey Unit 7 March, Chatteris and Whittlesey Unit 8 MASH MET Hub MST Partnership and Quality Assurance Policy and Practice PQA CP Team Private Fostering and Kinship

	Safeguarding North Safeguarding South SEND 0-25 SEND Cambridge City SEND East Cambs SEND Huntingdon and St Ives SEND March, Chatteris and Whittlesey SEND Cambridge South SEND St Neots and RSY SEND Wisbech Sexual Behavioural Service South Cambs Unit 1 South Cambs Unit 2 South Cambs Unit 3 South Cambs Unit 4 South Cambs Unit 5 South Cambs Unit 6 START Team Statutory Assessment Team North Statutory Assessment Team South Strategic Business Support Supervised Contact Service The Hub Virtual School Business Intelligence Team IS Training Team IT & Digital Team LGSS Appointee and Deputyship LGSS Financial Assessment Team LGSS IT Service Desk LGSS Application Support Mosaic Project Team Wisbech Unit 1

	Wisbech Unit 2 Wisbech Unit 3 Wisbech Unit 4 Youth Offending Services LGSS IT Service Desk Self Directed Support (SDS) SEND North SEND South Sensory Support Team 0-25
Where and how will the data be stored? *Include details for electronic and paper*	Data will be stored in Mosaic and Wisdom systems **Integrated systems -** Agresso, NHS Mini Spine and Address Gazetteer. **Paper** **Electronic Archive system**
Information sharing	
Will any information sharing take place? Please define the outline overall objectives of information sharing	**Yes** Statutory basis for data collection required by law Data collection and sharing is fundamental to the operation of the local authority, and/or necessary to provide services efficiently and effectively. Data output is fundamental to the operation of children's and adult services, and/or necessary to improve services and inform the public. NHS Number matching: a common code to identify a person across health and social care is a prerequisite for sharing care records. Electronic Referrals to Mosaic/ ASC using Fenestra portal gateway - TBC

	Child Protection Information System (CPIS): electronic interface between Mosaic and CPIS, which will share information for CP and LAC cohorts to unscheduled care settings Use of Mosaic to share information between MASH Partners Sharing information between directorates, services and teams (see list of organisations above)
Provide details of data that will be shared with any external organisation(s)	Core demographics and service and individual level data with MASH, CPFT – Mental Health, CPFT – Occupational Health, CPFT – health staff in Learning Disability Partnership, Carers Trust. (Access/Security permissions implemented part of project) CPIS Interface connecting Mosaic to the NHS Spine. This will be used to exchange looked after child and child protection information between Mosaic and NHS unscheduled care settings.
If information / data sharing required, is there an information sharing agreement (ISA)/ contract in place? If not please inform the IM team who will help you create one an ISA	Multi agency information sharing agreements within both directorates The list includes the following agreements: • Enhanced response • Immunisation • CDLRF • CLDP • Case Finding • Mash • Community resistance • ENCTS • EFA • Early years casey • MSDI • CPIS • Older peoples information sharing

	• Carers trust • Youth rehabilitation • Social care & YOS • Mental Health • Learning Disability Partnership • AOP • Troubled families • Count Every Adult Team • Community Navigators • Soft concerns • TCHC Youth contract • Electoral Registration • Free schools meals • TF nationally impact • Home fire safety checks
Does the sharing rely on consent to take place?	Mosaic system covers both Safeguarding and Early Help Services. There will be circumstances where information can be shared without consent and instances where consent will need to be obtained. Work is being progressed by the information and records team to ensure GDPR compliance in terms of consent for processing personal data.
Will ANONYMISED / PSEUDONYMISED INFORMATION/NON PERSONAL DATA be shared?	**Yes** Statutory returns

How is the information to be shared? Will the data be transferred? How will it be securely transferred?	**A** Xml, Xls DFE & NHS Digital secure collection portals
Information Security	
What information security controls have been put in place? • Give details of the access controls to be in place for staff accessing personal data. • IT security controls • Training and awareness	IT Security and password complexity etc. will be the same as that of the network i.e. change password every 3 months, passwords at least 6 character, must contain upper and lower case and alpha and numeric characters. All access is governed by the User Admin process using online forms. (We have yet to define the BAU process for access so I don't know whether it's just managers' approval or that you will require sign off from trainers). **Mosaic System** Security is defined by project System Admin controls and audit mechanism **Mosaic Training and awareness** The following will be covered in classroom training: Accessing information only for professional use. Not allowed to access information for personal reasons. Should a member of staff wish to access information they need to go through the Subject Access Request route. It is a disciplinary offence if anyone is accessing information for personal reasons. Sharing of log in details for Mosaic – do not to share log in details with anyone else. It is a disciplinary offence to log into Mosaic as someone else. Information Security – Importance of keeping information safe i.e. sending documents only to 'safe' email addresses.

	Information Security – Importance of keeping information up to date in Mosaic and in relation to the address for a family ensuring this is up to date so that we do not have an information breach i.e. sending information to the wrong address. **Mosaic elearning** Information Security/Sharing is also included in the Mosaic MeLearning which will be a mandatory module. Corporate Information Governance e-learning needs to be completed for all staff using Mosaic. **Policies and procedures** Confidentiality and Information sharing is covered more generally in the CCC Code of Conduct and our Information Sharing and Information Security Policies. **Mosaic System** Security is defined by project Sys Admin controls and audit mechanism.
Data Quality	
How will data quality be assured?	• Business process • Mosaic DQ reports in system • Internal controls • Business/data validation rules - to be considered in Mosaic • DQ reports • Data Cleansing

Records Management	
What processes are in place for managing retention and disposal of records? What will happen to the personal data when it is no longer required?	**Mosaic documentation** File Retention Criteria can be can be configured in Mosaic, and Retention Rules can be applied to individual records.
Freedom of Information	
What processes are in place to respond to Freedom of Information (FOI) requests?	FOIs and SARs are managed via the Business Intelligence I.R team. Information held relating to FOI requests will be extracted and analysed using the relevant reporting tools, primarily Business Objects, SSRS, Corius, Excel. SARs will be dealt with by the Business Intelligence I.R team.
Risk	
Are there any other risks to data/information security, privacy, risks to individual, compliance, associated corporate/organisation which needs to be highlighted?	Data storage and processing creates risk of confidential information being accessed without knowledge or consent of service users **Dependency on configuration of system** **Risk –** staff seeing information they shouldn't – Confidentiality. **Risk Control** –

	• Restrict areas to workers based on rules. Rules decided by services. Training and knowledge for staff so they know what they can have access to. • Restrictions – audit trail. Managers will have audit trails through IT reports. Basic audit reports can be requested. Change request audit report can be produced. Case history in records will carry an audit of changes made in the system. • Clearly defined responsibilities in the system. Inappropriate access report – highlighting Fraud. Worker roles – security will be configured – i.e. who can do what, appropriate role types. Staff training needed so they can understand their responsibilities, i.e. code of conduct. • Workflow data to right people, work will be allocated to staff. • Access to Staff - Add starters – restricted to a team, moves – authorisation of approval, finish. Linked to Active directory. Web logging. Controls – HR, movers work role associated with role. **Risk** – integrity – staff changing information which they should not be – **Risk Control** – Restricted access – profiles are see, view and add, view and alter, full access. Steps in procedure. Changing the information controls are covered in the training. BSO have same access rights as Team managers, role to allocate work is covered in the training. Information Governance training for all staff and it is covered in the Mosaic eLearning training. **Risk** – availability – security of the system. **Risk Control** – Technical – • Fail over, disaster recovery. • Netscalers. • Penetration testing – arranged for March, to test the overall IT security of the system. • LGSS IT and SLA – Servelec SLA. IT and Digital team – governance of systems

	• External users – two factor authentication. Log into the system – via CCC network. Security on boarding – to be fit for purpose**.** **Risk -** Collection of data - Principle 1 (fair and lawful processing) is breached – GDPR, processing the personal data. **Risk Control** – Info and records team working with services to ensure that processes are they compliant with Principle 1. **Risk** – retention of data – poorly defined – lack of data retention. **Risk Control -** Info and Records team working with services to ensure correct retention periods are used. **Risk –** system is not compliant with GDPR – **Risk Control** – implement 5.15 version – compliance. **Risk –** data quality is lacking **Risk control** – forms designed to have limited options in terms of data selection / input . Key drop downs. Data quality report – children's cohort. Mandatory fields. DQ – AIS system. Integration with NHS Mini Spine, DARS.

How are these risks mitigated?	See above. Identifiable data stored only where necessary and destroyed or anonymised as soon as no longer necessary. De-identifying data reduces or eliminates the risk of a person's identity being revealed and thus protects privacy.

IM checklist – to be completed by Information & Records Team

Is the purpose of processing the personal data listed in the organisational notification to the Information Commissioner?	Yes
Data Protection assessment – comments from the answers above. How could data protection be improved? Conditions in table 2 – processing as sufficient.	Covered in response above.
Information sharing assessment – comments from the answers above. How could data protection be improved?	Covered in response above.
Information Security assessment – comments from the answers above. How could information security be improved?	Covered in response above.
Data quality assessment - comments from the answers above. How could data quality be improved?	Covered in response above.
Freedom of information assessment – comments from the answers above.	Covered in response above.
Risks assessment – are risks sufficiently mitigated? What controls need to be introduced?	Risk and Risk controls have been listed
Overall assessment What needs to change?	Actions below need to be completed
Sign off - If acceptable, to be signed off by member of the Information & Records, CCC and responsible member of staff.	PIA signed off if actions below are completed.

Notes

Data controller: a person/organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what **information** is held, what is added and what is removed, how **information** is moved, and who has access and why.

Sensitive personal data , data which relates to sexual life, ethnic origin, medical information, religious beliefs, political views, criminal convictions

Processing - in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.

Data breaches - List the relevant policies. Incident reporting is included in the contract - yes/no, data sharing agreement yes/no?

Information security controls - IT requirements analysis. *Include details of functional specifications, security controls system architecture, compliance with ISB standards, selection of software, maintenance and replacement costs, support contract requirements etc.* Give details of access restrictions to building/areas/systems e.g. passwords/smartcards/ID cards etc. How will IT support be provided? Will this be provided from outside of the UK? If so, provide details of the security arrangements. Give details of the security systems in place that will ensure that PID is protected from unlawful or unauthorised access e.g. firewall, anti-virus etc? Give details of measures in place to protect data from accidental loss, destruction or damage? Will mobile devices be used? If so will they be encrypted?

Information sharing – Consent - How has consent been obtained/how will it be obtained? Arrangements for each partner and arrangements if consent for sharing is denied or withdrawn by an individual. Notes re: the likelihood of need to share without consent if relevant. Will explicit or implied consent be obtained from patients/service users? Is there a supporting Patient Information Leaflet? State method to be used to record consent /dissent. If consent is identified as the reason to legitimise processing what happens when consent is withdrawn? Are individuals offered the opportunity to restrict processing of

their personal data? If so when is that opportunity offered? Are procedures in place for maintaining an up to date record of use of personal data. If so how often and by whom?

Non – personal information - Set out any special basis for restricting the information shared. Any conditions that need to be met, notifications made, etc. Arrangements if conditions are no longer met. **ANONYMISED / PSEUDONYMISED INFORMATION** Set out any special basis for restricting the information shared. **Transfer of data -** Set out requirements specific to this sharing arrangement. What transit mechanisms are acceptable? What transit mechanisms are not acceptable?

Data Quality - What processes will be in place for data validation? Are national or locally defined data standards being used? Where different systems are recording the same data, are processes in place to ensure there are no inconsistencies between them? Who will have access to the system and how will that access be controlled? Will training on use of the system be provided and a list of trained personnel maintained? Is there a process in place to ensure all users have attended mandatory data protection training? List the IG training requirements for staff (this may be role specific). Is IG training mandatory? Has/will the requirement to complete annual IG training been included in the contract? Is there an active audit trail built into the electronic system used?

Records Management - Does the contract include requirements relating to records retention and disposal? What will happen to records at the end of the project/service? Has reference to handover of service user records to new provider been included in the contract?

Appendix 1a Data Extract

Person identifiable information extracted: Names; dates of birth; addresses; NHS numbers; NI numbers; unique pupil numbers.

Data will be extracted from the SWIFT/AIS database for the Adults Services data migration and the Capita One database for the Children's Services migration. Data will be extracted from SWIFT/AIS directly into the Mosaic database. Data from Capita One will be extracted to an intermediate database holding the data warehouse for the Children's Services migration and from there into the Mosaic database.

No data will be deleted from the source databases by the migration project. Records will be deleted as part of the business as usual process once the system is live according to the data retention policies that apply to the people concerned.

The data extracted will be used in the same way that is already being used in the existing systems – to identify clients of Adults and Children's Services and their relatives.

Currently just over 48,000 people are being migrated as part of the Adults Services migration and 444,000 as part of the Children's Services migration.