



DPIA – Integris MIS (for schools procuring via Derbyshire County Council)

Version 1.0

Name of School/Trust	Chinley Primary School
Document Prepared by	Data Protection Officer and Peter Lambert
Reviewed by DPO	
Date of DPO review	
Governor minute number/reviewed by SLT	Reviewed by SLT
Governor/SLT review Date	12.01.2024

Version History			
Version	Date	Detail	Author
1.3	August 2023	DPIA template revised to reflect changes to ownership of the MIS system. Reference to DPIA completed by Derbyshire County Council. Updated throughout.	Claire Archibald, Data Protection Officer

Introduction

Integrus MIS (Integrus) is a Management Information System (MIS) that allows the recording of staff and student details, attendance recording and monitoring of pupils, communication with parents and carers of pupils at a school by text or email, information regarding meals purchasing and can also hold staff information.

By using this system, the school aims to achieve the provision of a convenient and secure method of communication, pupil attainment tracking and attendance monitoring, provision of timetabling and staffing information. The system will save staff time in inputting information in multiple systems, provide more accurate reporting and centralised data points to improve accuracy. The system allows the school to generate a range of reports, including details of individuals and personal details.

Chinley School understands the scope of functionality which Integrus provides however its use is limited to recording of staff and student details; attendance recording and monitoring of pupils; information regarding the purchasing of meals and a database for contact information.

Integrus also have "Integrus Datashare" - this is an API tool to share data easily and securely from Integrus with third party service providers and local authorities. The school has full control over which of Integrus Datashare partners are given access to data. Integrus provide information in relation to this tool at <https://help.integrus-education.com/integrus-datashare>. This DPIA does not consider the suitability of this datasharing, as a DPIA into any of the linked partners would include consideration of the sharing via the Datashare functionality. It is noted that one of the partners is Wonde; the DfE have requested that schools share data with Wonde from their MIS as part of the Attendance Sharing Scheme. Whilst the school would carry out a separate DPIA into any external data sharing via Datashare and/or Wonde, it is clearly anticipated by the DfE that schools should share data from their MIS externally using such methods.

The school procures Integrus via Derbyshire County Council (DCC), who procure it on school's behalf. The school has an [End User Licence Agreement \(EULA\)](#) with Integrus. DCC is involved in three different capacities in relation to the use of this platform:

1. DCC has a contract with Integrus to supply licences to schools on a traded service basis which schools can then choose to procure- schools are their own data controllers but they do rely on DCC to have carried out the appropriate due diligence on the platform on their behalf;
2. DCC provides a support team to assist schools with the usage of the platform which involves some DCC staff accessing personal data as a processor to assist school staff;
3. DCC also receives some personal data from Integrus who extract it from the system in relation to suspensions (previously known as fixed term exclusions). DCC would receive this information anyway via the DfE and the Census process, but this information is received earlier and more frequently which allows DCC to fulfil its obligations in a more effective and prompt way (particularly in relation to children who may be missing from education) and minimises the work and any data security concerns of the school sharing this data with DCC via other manual methods.

Schools are not obliged to use Integrus or procure it via DCC. The majority of Derbyshire primary schools, Pupil Referral Units and special schools do choose to procure Integrus this way. Additionally, a handful of schools outside the Local Education Authority also choose to procure Integrus and the associated training and support provided via DCC.

DCC does access some information and act as Data Controller for some personal data extracted from Integrus in relation to pupil suspension and census data for Derbyshire maintained schools. The council is required by law to receive this information from schools and by taking it directly from Integrus allows the council to keep

this information up to date and reduces administrative burdens and technical difficulties. Other Derbyshire schools who do not use the system are still required to share this information with the DCC, via manual methods. A [Data Sharing Agreement](#) is in place between the Council and Schools in relation to this automated extraction.

The DfE provides some [guidance for schools](#) in what to consider when selecting a MIS which includes Integris. There are other providers of school MIS systems available, but DCC only offers procurement and support for this particular provider. DCC also offers extensive guidance to schools on how to use the Integris system, what to input and how to keep the information secure.

In October 2022, DCC completed a DPIA for this software system. As part of that work, it was identified that the DPIA should be shared with schools who purchase Integris via DCC. The DPIA identified that schools are also responsible for conducting their own DPIAs into the system. Subsequently, in 2023, Integris (which was owned by RM Education) was then acquired by another company, The Key. This school DPIA takes into account the DCC DPIA and the new ownership of Integris.

This is the first time that the school has completed a DPIA for Integris.

Describe the nature, scope and context of the data processing

Whose data will be collected?

Children's, staff, parents and carers personal data will be collected.

Student data may include:

Forenames, Surname, Alias, DOB, Gender, Groups, Dietary Requirements, Postal Address, Identifiers, Meal Selections, UPN, special Education Needs, Pupil Premium & FSM status, Photograph, Ethnicity, preferred pronoun, Family links, Year Group, Class, House, ULN, UPN, Transport Information, Learner Funding & Monitoring, YSSA agreement, enrolment details, school history, Adult Contacts details, Pupil Contact details, Groups, Behaviours, medical Disability, Exclusion, Funding Indicator, pregnant mother, (religion for some schools), (DAF for nursery settings), Service child, EYPP basis for funding, care order details, post looked after arrangement, education supervision order, language (nursery – hours at setting, funded hours, 30 hour code, extended hours) Young carer, traveller status, medical details affecting school, other unique fields as defined by the school, statutory and non-statutory assessment data

Parents/carers data may include:

Title, Forename, Surname, Salutation, Gender, House Name, Street, Locality, Town, Postcode, Work Telephone, Home Telephone, Mobile Telephone, Email, relationship, FSM applicant, NI Number, DoB, parental consents.

School Staff / Governors / Volunteers (or anyone working in the school especially if using the Integris Single Central Record) data may include:

Title, Forename, Surname, Gender, Username & Password for the MIS, DOB, Gender, Groups, Salutation, Dietary Requirements, Medical Information, Postal Address, Identifiers, Payroll number, National Insurance number, Salary details and role specific details. Contacts, other unique fields as defined by the school, Qualifications, QTS status, Training, Medical details, Cover availability and Periods covered, Clearance data.

It is also possible to keep basic financial accounts (school meals) for individual students and staff.

Note that the list above is not exhaustive and may change from time to time as products and services evolve. Please see [information audit](#) for details of all personal information capable of being held within Integris.

How will the data be collected?

The data is collected using a variety of methods. The first entry point is when a child joins the school - at this point, information is collected from their parents/carers (using details taken from admission forms) or from a previous school (via CTF). Thereafter, information is added to by staff at the school depending on their role. Parents/carers are regularly reminded to update the school with any amended or new information (e.g. regarding any allergies or other information). Data will go through an accuracy check with parents/carers and staff / governors / others working in school on an annual basis. Parents may submit information using a Microsoft Form link sent to them through Parent Hub.

What is the lawful basis of the processing of this data?

Inclusion on the school MIS is compulsory for pupils. Schools are required to process this personal data under a range of applicable legislation including The Education Act 1996, The Education (Pupil Registration) (England) Regulations 2006 and The Education (Pupil Registration) (England) (Amendment) Regulations 2010, 2011, 2013 and 2016. The School Attendance non-statutory guidance gives further detail on the schools obligation to process pupil attendance and contact information. The Keeping Children Safe in Education statutory guidance gives information about recording attendance and other information about children (such as their home address, contact details and family details).

Information relating to staff employed by the school is also included in the Integris system.

Information may be retained relating to medical conditions or allergies that may be required in the event of a medical emergency.

Information may be given of other data subjects who are the 'emergency contact' for the child - this information is given by the parents who would be responsible for obtaining the agreement of the data subject for the school to hold this information.

Information may be provided by parents as part of transactions for school meals or trips.

The lawful basis for the school processing this data therefore depends on which data is captured - the lawful basis may be Article 6 of the UK GDPR (letter in brackets relates to the UK GDPR):

- 6(a) consent
- 6(c) legal obligation;
- 6(d) vital interests of the data subject; or
- 6(e) public interest.

In relation to special category data, the relevant legal basis may again vary, but may be Article 9 of the UK GDPR (letter in brackets relates to the UK GDPR):

- 9(2)(a) explicit consent;
- 9(2)(b) obligations in the field of employment and social security and social protection law;
- 9(2)(c) vital interests; or
- 9(2)(g) substantial public interest.

Who is data controller and processor?

The school is the data controller and Integris is the data processor.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Information contained within Integris will be shared:

1. With other schools where a pupil moves to a new school (this may be at a standard transition point, e.g. from primary to secondary school) or at non-standard points where a school move is necessary or required by the pupil. Information will be extracted from the Integris system and sent as a CTF file via the DfE 'School to School' system. This sharing of information is a statutory requirement under section 9 of The Education (Pupil Information) (England) Regulations 2005.
2. With the DfE for Census collections- schools are legally obliged to do this by The Education Act 1996, Section 537A.
3. With parents/carers, solicitors (or other people authorised to act on behalf of the data subject) who request a copy of the information contained within Integris. This may be requested under The Education (Pupil Information) (England) Regulations 2005 or under the UK GDPR as a Subject Access Request.
4. With police or other law enforcement agencies where the school is required to do so, for example, pupil attendance data may be required in relation to investigations of fraud or penalty notices relating to non-attendance.
5. With Derbyshire County Council:
 - a. With DCC staff who provide technical support to schools who use the Integris system. These staff are based within the Education Data Hub and will automatically be set up with logins for each school account. This enables staff to assist school staff with any technical issues they have as they will be able to see the data from a school's perspective. These staff are only authorised to view the school data when requested to do so by the school and a log of access records is automatically created.
 - b. Data is extracted from Integris relating to pupil suspension. The council are required to collect this information by law and a data sharing agreement is in place- see above.
6. With Integris for the purpose of customer and technical support queries. This is set out in the End User Licence Agreement (between Integris and the School). Staff accessing the data for support purposes are all based in the UK. For development purposes, if the UK team cannot resolve a technical issue then it may need to be escalated to colleagues based in India. This is addressed in the EULA (clause 7.8).

How long is the data kept for?

No data is deleted from the Integris platform, unless carried out by the school. The school should therefore retain and then delete data in line with their normal records retention policy. Schools that purchase Data Protection Officer services from the Education Data Hub are provided with a template records retention policy, which includes guidance on how long to retain pupil and parent records within the MIS system. Generally, once a child has left a school, all records should be transferred to the school that the child moves to, unless the school is the "last known school" for that pupil. These issues are dealt with in more detail in the Record Retention Policy.

The Retention Policy was reviewed in January 2024 as pupils all move on to their next school no reference was made to the retention of data as all information is passed to their next school. Specific guidance is recorded in the policy related to safeguarding and children protection records (see Retention Policy).

Data is only retained by Integris for the length of the contract with the school. No backups are maintained by Integris or by DCC after the end of the contract. Therefore, the school would need to arrange to download any data, or to continue to pay Integris to hold data for them if they decided to end the purchase of the system.

How and where will the data be stored?

Data will be stored on an online hosted platform which is hosted in Microsoft Azure using the latest SQL database technology. The hosting for Integris will remain within the EEA. During the duration of the contract, data is backed up by Integris as set out in their guide at <https://help.integris-education.com/how-and-when-is-integris-data-backed-up>.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? If yes, please describe the new purpose below.

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?

No action or decisions will be taken against individuals as a result of using Integris itself. The information may contribute to decisions about matters such as penalty notices imposed on parents who fail to ensure that their child regularly attends school.

The system does contain capability for some basic profiling of academic progress and attainment through the reporting functionality of the system (Insight). This allows the school to produce reports on a number of fields which may enable the school to conduct some profiling. For example, the system may be used to identify “pupil premium boys with low KS1 attainment and poor attendance” and identify these pupils for extra teaching intervention. This information can then be used as an additional tool by schools to identify pupils who need additional support. The school would use a variety of methods to select pupils (the main one being working with the relevant staff who work with pupils and know their attainment/needs well) and this basic profiling would not be the only means of selecting pupils for additional support. Therefore, the use of the system and any reporting functionality will not be processing should not have a significant impact on data subjects. The school is aware of the requirement to balance the needs of the leadership team to use data to measure the performance of the school against the requirement to protect their data subjects.

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, information will be retained on a large-scale regarding pupils, who are considered to be vulnerable data subjects. Integris will be used as the main Management Information System for pupils in the school. The nature of the data subjects (children, therefore classed as vulnerable data subjects) and the data about them will include information that is particularly private- including their health status, SEN status, Pupil Premium Status (which may be an indicator of household deprivation), religious beliefs, ethnicity, educational attainment and behavioural information (including any exclusions).

Similarly, sensitive data may be retained on the system about staff, as described above. This information if released, or lost, could raise privacy concerns.

Note regarding Consultation

The school/trust will consult with the Data Protection Officer and Governors/The Academy Trust Board.

The school have been supported with the completion of this DPIA by the DPO. The DPO also works for Derbyshire County Council and supported the council with the preparation of the DCC DPIA- this document is embedded in the due diligence section below for the school data protection staff/governors' information.

Identify the privacy and related risks and mitigations

Data Protection Principle	Description and mitigation in place	Further mitigation actions that must be carried out by the school	Risk status after mitigation actions completed	Person responsible and if applicable, date of completion
Lawfulness, fairness and transparency .	The lawful basis for the sharing of data will vary and will depend on the data processed - see above for full details.	None	No risk	n/a
	The processing is fair-sharing personal data in this way is fair (and expected).	Remind parents that they should let other emergency contacts know that their information has been passed onto the school for this purpose- this could be included as a note in the admissions paperwork that parents complete.	Minimal-accepted	Peter Lambert
	Data subjects have a right to be informed - the processing will be transparent if the school ensures that the relevant Privacy Notices are updated to include information relating to this processing activity.	Ensure relevant Privacy Notice(s) are updated.	Minimal-accepted	Peter Lambert
	Data Subjects must be able to exercise their rights under data protection laws. The rights are already available to data subjects and are explained in the privacy notices- these rights are extended to the data processed on the Integris system.	Ensure that the privacy notices are up-to-date and easily available for data subjects (e.g. on school website). The DPO supports the school with addressing any data subject rights requests. Integris provide guidance in relation to Subject Access Requests Student and Staff: https://help.integris-education.com/introduci	Minimal-accepted	Peter Lambert

		ng subject access request https://help.integris-education.com/generating_a_staff_access_request		
Purpose limitation.	Personal data will be shared for the purpose of this processing activity- the school will not use the personal data for any other purpose beyond what it already does or reasonably needs to in pursuance of ensuring pupil attendance, safeguarding and other administrative purposes. Integris has confirmed that personal data will only be used for this purpose and no other.	School/Trust relies on external providers documentation giving assurances regarding the processing of personal data for this purpose only.	Minimal-accepted	n/a
Data minimisation	Personal data shared is as set out above. The school deems these data sets as the minimum needed for the purpose of processing.	Review data sets collected and check regularly. Keep this under review.	Minimal-accepted	Peter Lambert
Accuracy.	The school is responsible for ensuring personal data is accurate and up to date. All staff have a responsibility to ensure that data is factually correct.	Nominate member of staff responsible for ensuring personal data is regularly checked for accuracy. Any errors in personal data identified are referred to the Admin Officer who will check with parents and initiate changes.	Minimised- but risk remains if data subjects do not let school know their information has changed- this must be kept under review.	Marion McCabe
Storage limitation.	Storage of this data is already addressed as part of school retention policies. Integris state this data will be retained for the length of the contract / archive Schema contract and then deleted on the Schemas. The annual	The school is the data controller and can delete data from the system using the correct administrative accounts. Ensure staff member deletes or destroys data no longer needed- whether stored on	Minimised- but risk remains if school staff do not take proactive steps to manage retention of data. This	Peter Lambert

	back-up are kept for 9 years. https://help.integris-education.com/how-and-when-is-integris-data-backed-up	external services or internal systems- this must be done in line with the school retention policy.	must be kept under review.	
Integrity and confidentiality (security)	There is a risk that this processing could result in a data breach that either staff at the school, or the external provider could be responsible for. The impact of such a data breach would potentially be very high as the data relates to children who are vulnerable data subjects. Examples of risks: *Motivated intruders may try to hack the system to access personal data *Staff may accidentally share personal data with the wrong person *Personal data may be accidentally or maliciously deleted *The processor may not have appropriate measures in place to safeguard the personal data. A Data Processing Agreement is necessary for this project. The law states that this document should contain key terms. The checklist in the Appendix sets out which terms are required and where they are in the documentation. Reasonable due diligence has been carried out into	Ensure all school staff comply with general data protection and cyber security instructions and guidance when using school systems. Remind staff that the information in Integris is sensitive and ensure only the appropriate staff have access to the minimum level of data required for their role and that passwords should be kept secret. Ensure staff accounts and levels of access are kept up to date. Promptly remove users from the system when they leave the school (inactive users are deactivated after 60 days and must be reactivated if still required). Staff error is the main reason for data breach when sharing data externally- DPO regularly trains staff, but school leadership should also regularly remind and support staff to ensure that they process personal data with care and attention. Cyber-attacks are another high risk to schools- it is important that staff follow guidance and instruction given to them	Minimised- but cyber security remains a high-risk area for all schools- this must be kept under close review.	Peter Lambert

	the suitability of Integris and they have provided some information about security - see Due Diligence section below. Integris does not currently have ISO 27001 certification- this has been reported by the School DPO to the contract managers at Derbyshire County Council for investigation/resolution. The school is responsible for ensuring their staff comply with Data Protection requirements. Integris is also responsible to the school under the terms of the EULA.	to minimise the risk of cyber-attack. Ensure that features such as 2 Factor Authentication for the platform are enabled wherever possible (this is currently only available if school is using RM Unify). Check the DCC DPIA and due diligence section below - the school leadership must be satisfied with the information provided by Integris and DCC.		
Accountability.	All parties have responsibilities to account for their data protection practices. This DPIA and the documents referred/linked to in this document form part of the accountability practices of the school.	Retain evidence of work done to comply with Data Protection laws. Add this new processing activity/supplier to the Information Asset Register (RoPA) (in the Suppliers Tab of GDPRiS). Whilst there have been no issues with the use of Integris so far, there may be continuing risks that are not yet fully known, particularly in relation to any new functionality. Therefore, it is important to keep this DPIA under review over time as understanding of the risks and use of the platform and the way that data is processed will change in the future.	Minimal-accepted, but keep DPIA under review over time and as use/staffing changes.	Peter Lambert

		DPO to review this DPIA and check that the school have completed it correctly.		Data Protection Officer
--	--	--	--	-------------------------

Risk Rating Decision

As a result of the privacy risks and mitigations it has been evaluated that the overall level of residual risk to privacy after the mitigation actions have been carried is low/medium. The school leadership and governance should note this risk and if appropriate, include it in the Information Risks section of the School/Trust Risk Register.

Appendix A: Evidence of due diligence

As the Data Controller, the school/trust may only rely on Integris if it provides sufficient guarantees in relation to appropriate controls and GDPR compliance. The statements at the weblinks and embedded documents below have been checked by the School and the Data Protection Officer:

External Provider Name and Address	The Key Group 103 The Key Support Offices 8 th Floor HYLO 105 Bunhill Row London EC1Y 8LZ
External Provider DP Contact Details	Damian.brooks@arbor-education.com
Privacy Notice	See link below
Contract/Data Sharing Agreement	See link below
Terms of Use	See link below
Any additional information	End User Licence, Terms and Conditions and Datashare Agreements (integris-education.com) DPIA produced by DCC:  2022 04 05 Data Protection Impact Ass The DPO requested that Integris complete a Request for Security Information Document. This is embedded here for the school to reference:  Integris Security and Processing Request fc The email below gives further detail in relation to the security questionnaire and ISO 27001 accreditation: From: xxxx@integris-education.com> Sent: 01 September 2023 18:16 To: [DPO details] Cc: Subject: Completed DPIA for Derbyshire County Council Good afternoon, I am now pleased to attach the completed documentation. This has been compiled with the help of our Development Team Manager, who as you would expect,

	oversees the day to day running of Integris with appropriate accountability together with the DPO for The Key Group. As I explained on the call, up until recently RM retained accountability for the day to day running of Integris whilst our Development Team are in the process of transitioning to The Key Group. With this transition nearly complete, we recognise that we need to update our ISO credentials to reflect that Integris will now be operated by The Key Group. I am currently advised that this is likely to happen in March 2024. Just to reassure you, there will be no operational changes as part of the full transition to The Key Group. We continue to work to the same standards and processes as we did under RM, with the same team of people (including management structure) working to those procedures. Derbyshire County Council are known for being outstanding in your data protection services to schools. As such, despite my assurances, I anticipate you may have some questions or concerns. I'd be happy to arrange a call with members of the Senior Leadership Team of The Key's MIS division and our DPO, where we can explain more about governance and practices which are common across the group. Do let me know if you would like to explore this further and I can get this arranged. If you have any questions at any point do come back to me. Take care, [name] Partner Relationship Manager, Integris Education  Integris MIS  Arbor Finance E: xxxxx@sesl-education.com M: TBC W: www.integris-education.com Schools Educational Software Ltd, Floor 8, HYLO, 103-105 Bunhill Row, London, EC1Y 8LZ
--	--

Checklist for Data Processing Agreements

A Data Processing Agreement must set out:	Included in the EULA
The subject-matter of the processing	Schedule 1
How long the processing will continue for	Schedule 1
The nature and purpose of the processing	Schedule 1
The type of personal data	Schedule 1
The categories of data subject	Schedule 1
The controller's obligations and rights	4
The processor will only process the personal data in accordance with our written instructions, unless required to do so by law	7.4.1
The processor must obtain a commitment of confidentiality from anyone it allows to process the personal data, including staff, agency workers and volunteers.	7.4.3
The processor must put in place appropriate technical and organisational measures to ensure the security of any data they process	7.4.2
The processor must assist the controller and also to take "appropriate technical and organisational measures" to help the controller respond to requests from individuals to exercise their rights.	7.4.4
The processor will notify the controller of any personal data breach without undue delay	7.4.5
To assist with any Data Protection Impact Assessment	7.4.4
The processor to provide the controller with all the information that is needed to show that the obligations of Article 28 have been met; and	7.4.8
The processor to allow for, and contribute to, audits and inspections carried out by the controller, or by an auditor appointed by the controller.	7.4.8
at the controller's choice, delete or return to the controller all the personal data it has been processing for it; and	7.4.7
delete existing copies of the personal data unless EU or Member State law requires it to be stored.	7.4.7a
The Processor must not use another processor (a sub-processor) without the controller's specific or general written authorisation	7.5
If a sub-processor is engaged, there must be a contract in place which gives effect to terms substantially similar to the one between the controller and processor	7.7.1
if a sub-processor is employed under the controller's general written authorisation, the processor should let the controller know of any intended changes and give the controller a chance to object to them	7.6
The processor is liable to the controller for the sub-processor's compliance with its data protection obligations	7.10