GDPR - Data Mapping – Good Shepherd Primary Catholic Voluntary Academy

July 2019

ADVICE ON DATA MAPPING

Now that GDPR is in force, one of the most important tasks that you need to do is to map the personal information that you hold and share as an academy. To support schools with this task, rather than start from scratch, this largely completed Data Map template has been compiled, detailing much of the information generally held in schools.

We are aware that some of you have already made use of mapping tools provided by other organisations, so you do not have to complete this tool if you have already captured all the information using a different tool.

As you can see, the Data Map has been split into a number of categories such as Pupil Admission data, Assessment data etc. This list is by no means exhaustive and should you hold other information not listed here, then please add this to your Data Map template accordingly. Alongside the data we must also explain how you obtained that information, the justification for holding it, where is it held/stored, and what risks exist in relation to you holding and using the information.

In addition, for any information that you share with others, or hold on external servers, you also need to set out the legal justification for sharing personal information with that service or agency and where it held.

Personal data is defined as any information which relates to an identified or identifiable person, and which either identifies that person or, in conjunction with other information held, allows a person to be identified or categorised in some way. This will therefore include all of the following information, plus much more:

- Name, Address and Contact Details, Job Details, Date of Birth, Educational Record, including Special Educational Needs, Medical Information, Safeguarding Information, National Insurance Number, Gender Identity.

Data Source relates to where each type of information comes to you from. It is likely that data of a similar type will be received from similar sources, so for example names of children to attend the school will come initially either from a local authority's admissions service or be provided directly by parents. Contact details for family members will usually come via a data collection form completed by parents. SEN information may come from other schools or from internal or external assessments. If there are multiple sources, list all the likely ones in this column.

Legal Reason/Basis for Processing - GDPR requires a legal justification for the holding and sharing of all personal information. Therefore, for each type of personal data you hold, and for each agency / service you share it with, you need to be able to explain why the law allows you to do so. Under GDPR, you need to be able to prove one of the following in relation to standard personal information such as names, addresses and dates of birth:

- Consent has been given;
- Necessary for the performance of a contract to which the data subject is a party;
- Necessary to comply with a statutory or other legal obligation;
- Necessary to protect the vital interests of the data subject or another person;
- Necessary in the public interest

Data Mapping

Please note that the justification of holding and processing information for the purposes of 'legitimate interests pursued by the controller' is no longer available to a public body such as a school or academy (the new GDPR does not allow this), which means that - unless consent has been given, a child is at risk, or a legal obligation applies - it is very difficult to justify the holding or sharing of personal information about a person.

For '**special' categories** of personal information, the rules are even tighter. 'Special' personal data includes any information which reveals:

- racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

This might therefore include some staffing information, and also information of a sensitive and personal nature about pupils, such as some special educational needs and medical information. In these circumstances you need to be able to explain why the law allows you to hold/share the information (i.e. which one of the five legal reasons above applies) and also prove one of the following reasons applies:

- Consent has been given;
- Necessary in relation to specific employment and social security legislation;
- Necessary to protect the vital interest of the data subject or another person where the person is incapable of giving consent;
- Personal information has been made public by the data subject
- Necessary in relation to legal proceedings;
- Necessary for reasons of substantial public interest;
- Necessary for medical or social care or public health reasons.

Data Storage: It is vital that you keep personal information secure, whether it is held in paper form or electronically. Therefore, you must set out how information is held internally and how it is transferred to and then held by external agencies, to the best of your knowledge. This should be straightforward for information held internally but may require research for external systems, in particular where they are web-based. Where is the server located for these services? Is it in the UK, elsewhere in the EEA, in the United States, or even somewhere else in the world? This will have particular implications as data security law is different in different parts of the world, but you need to be assured that standards applicable in the UK apply.

Risks: It is important that you give thought to risks associated with the holding, using, transferring and sharing of personal information. Could it get into the wrong hands or be used for the wrong purposes? What safeguards have you put in place? Your DPO can support you in the process of understanding risk.

Who has access to the Data: You need to identify which individuals or categories of staff within your academy have access to the data.

Data Sharing: if you share the data with external bodies. If shared externally, you need to list each of the external agencies and organisations that you share information with. This will include public sector bodies including local authorities, central government (particularly for academies) and the NHS, but also external contractors who provide educational services both in person (such as specialist teachers) and online (electronic communications systems etc.). All web-based systems will need to be included if they hold any pupil, parent or staff information inputted by the school, but do not need to be included if the school never input any personal information into the system themselves (including names of pupils or staff).

Data Mapping

Please be aware that your final Data Map will be reviewed as part of the Trust's annual GDPR Audit.

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Pupil Admission	Pupils Nursery Pupils Year1 to Year 6 Pupils Year 7 to 13 Different Types of Admissions • Nursery • Yr1 to Yr6 • Yr7 to Yr11 • Yr12 to Yr13 • Mid-Year Parents/ Carers	Personal Data: Name, DOB, UPN, ULN, address, contact details [Parent/Carer phone and email], free school meal requirements, doctors practice, language, Traveller status, country of birth, school history, attendance data, assessment results, exclusion history, photographs, CCTV Images, Post-16/UCAS/Bursary information Special Category Data: Medical/Dietary information, medical events, ethnicity/national identity, religion, SEN information, Gender, welfare details [in care], Safeguarding files Parent/Carer information collected – Name, address, relationship to pupil, phone and email. **Source –** Previous school, parents/carer or pupil • Y6 to Y7 – Info from LA admissions or previous school via CTF transfer • Mid-Year parents/carer complete information sheet. • College – former school or college/students/parents/carer provide information **Basis –** Statutory requirement for Census returns. Medical, Dietary, safeguarding and parent/carer contact info is in vital interest of the individual - Consent for School Catering Systems Biometric information	On/before admission to the school and can be updated by parents/carer during time at school. Shared with or used by: • Shared with school staff dependant on role in school to allow them to carry out their duties i.e. Teachers, Head of Year/Dept., data team • Added to School Management Information System (MIS) so pupils can be added to classes etc. and to enable full use of MIS Functions • Letters to parents/carers to confirm place and details, provide information about open days etc. • With the LA to confirm applications/ranking/places offered etc. • School transport • School catering system • School caterers re: dietary needs purposes • Medical Professionals incl dental support worker/services, Integrated Specialist Services, NHS, School Nurse To have/put 3rd Party Data Sharing Agreements in place if applicable Retained for periods as defined in retention schedule & CCTV Policy	Management Information Systems: Holds all pupil data gathered during admissions process Paper files are obtained from previous school or created and kept in school Pre-admission files from LA are received via spreadsheet and saved in secure folder on network Staff can export details from MIS and save on own network Cloud MIS OneDrive/SharePoint All these are stored on school servers MIS is internally hosted School networks are internally hosted and staff only have access to required areas **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	High risk to pupils as we hold a large amount of personal and sensitive information	Approx. 60 new pupils per year Hold data for approx. 410 current pupils Past data retained in line with retention schedule

Data Mapping

Purpose	Whose data	What data – Type of Data Source of data Legal basis	When it's collected Who is it shared with & why How long is it retained & why	Where it is stored? *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	Potential Risks	Amount of Data
Assessment Information	Pupils	Results of internal and external assessments, target grades, current levels, predictions, attitude scores, homework scores, coursework completion etc… Used to produce reports to parents/carers and analysis files for class teachers, heads of department and senior leadership to use. This is for monitoring progress of pupils. This information is filterable by key groups to allow trends and patterns to be identified. External examination results received from previous school for assessments done prior to admission and from examination board for exams sat whilst at school. Students joining college provide evidence of their previous exam results. Teachers will regularly conduct assessments in lessons. Previous KS1, 2 and 3 assessments are available via secure DfE website. **Source –** Exam Boards, Previous schools, DfE, Parents/Carer, Students and teachers **Basis –** Public interest, statutory requirement to report to parents/carers annually and performance of a contract. We will need consent to share pupils examination results with parents/carers from GCSE on.	Previous assessment results are collected on admission to the school. Internal assessment data is generated at regular intervals during the year to monitor pupil's progress. Shared with or used by: • Staff for monitoring purposes • Curriculum Tools – Dashboards, Management Information System. Additional analysis for staff and access to report for parents • Parents via reports • MAT for comparison and support • Local Authority statutory returns • Exam Boards required for examination entries • DfE via the examination boards • Ofsted via the DfE • Other schools for leavers • FFT for target generation To have/put 3rd Party Data Sharing Agreements in place if applicable Generic Headline data shared with Governors via Secure Trust Governor System Retained for periods as defined in retention schedule	Assessment data is stored in Management Information Systems, on spreadsheets and in paper files. Staff have access via MIS and other curriculum tools, dashboards. Files are saved on internal network. Data will also be added manually to pupil text books and staff planners. Cloud Systems Eazmag Pira & Puma **Security Measures**: • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	Medium risk as assessment data is not sensitive personal data. Emotional damage if results are shared without pupils knowledge	Approx 410 per year and data for previous pupils

Data Mapping

Purpose	Whose data	What data – Type of Data Source of data Legal basis	When it's collected Who is it shared with & why How long is it retained & why	Where it is stored? *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	Potential Risks	Amount of Data
Access Arrangements & Special Consideration	Pupils	For access arrangements pupils ability for reading, writing, processing etc… is assessed and documented on an application form along with their personal details i.e. name, DOB For special consideration an application has to be made with pupils name and other personal data i.e. DOB along with the reason for the request. This could be medical, family turmoil, distress etc. **Source –** Parents/carer, Pupils and teachers **Basis –** Legal obligation to assess pupils for additional needs and make applications as appropriate. Public interest for special consideration as pupils are entitled to have and disadvantages considered when exams are being marked.	Access arrangement assessments are carried out at the beginning of Year 6 and as and when a need is identified by teachers or parents/carer. Special consideration forms are completed after the exams concerned. The information is shared with the JCQ and examining bodies to enable them to process the requests. To have/put 3rd Party Data Sharing Agreements in place if applicable Retained for periods as defined in retention schedule.	Stored on MIS and school network. DFE website. Information is also loaded onto secure exam board websites which is external. **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	High as some information could be sensitive personal data. Details of learning difficulties and reasons for special consideration could cause emotional distress.	Approx 1 request per year

Data Mapping

Purpose	Whose data	What data – Type of Data Source of data Legal basis	When it's collected Who is it shared with & why How long is it retained & why	Where it is stored? *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	Potential Risks	Amount of Data
School Trips	Pupils and parents/ carers	Pupil Personal data may be taken from MIS i.e. Name, DOB etc… Medical information is requested on the reply slip/Parental Consent Form which accompanies school trip letters For residential trips parents must complete an additional consent form with medical and contact details. For international trips we require passports and EHIC cards. **Source –** Individuals/parents/carers **Basis –** we need consent for additional information and EHIC. Passports are a legal obligation.	Collected prior to any trips taking place. Information is accessible to appointed Trip Leaders and possibly to Staff attending the trip as well as emergency contacts who may work for the Trust – this is a designated contact for people on the trip. The trip provider may need to be informed of key information (such as medical/disabilities etc.) about the pupils to facilitate the trip. To have/put 3rd Party Data Sharing Agreements in place if applicable Retained for periods as defined in retention schedule	Information is stored on trip management system. Cloud Systems Planning info also stored on staff computers. Print out of registers and hard copies of parental/carer consent forms containing important contact/medical/dietary information may be taken on trips – to be securely transported by Trip Leader **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	Parental/carer consent forms could be misplaced whilst moving around on a trip. It is deemed that the risk of being unable to contact parents/ carers or being unable to provide relevant emergency care as outlined in these documents outweighs the risk of misplacing the documents – however, Trip Leaders and accompanying staff should demonstrate due diligence in keeping this data secure at all times	Varies per trip

Data Mapping

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Cashless Catering	Pupils and staff	Pupil names and DOB taken from SIMS. **Source –** Individuals/Parents/carers **Basis –** Consent	At installation of cashless system and then on admission to school. Cashless Catering Provider. (Squid) Who provide the software but have no access to the personal data unless we give remote access to help with issues. Appropriate staff in school have access to the management of the software. To have/put 3rd Party Data Sharing Agreements in place if applicable Retained for periods as defined in retention schedule.	All personal data is stored on an internally hosted server. Primary Cloud based Squid **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	Sensitive data being lost or accessed without authorisation	For all current pupils and staff approx. 450

Data Mapping

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Parental/ Carer Payment System	Parents/ carer	Parents/carers login to an account and can store their bank details to facilitate payments. **Source –** Individual **Basis –** Consent	When parent/carer signs up. Data is only accessible to parent/carer i.e. bank details Account deleted when pupil leaves or if parent/carer chooses to. To have/put 3rd Party Data Sharing Agreements in place if applicable Retained for periods as defined in retention schedule	Squid – stored externally Cloud Based data not process by Trust **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	Parents/carer card details being accessed Money manually added to wrong account	All parents/ carers can have access

Data Mapping

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Counselling	Pupils	Name, address of doctor's surgery and doctor's name, details of medical conditions and dietary requirements. **Source –** Individual/Parents/carers/Medical Establishments **Basis –** Vital interest or consent	School Nurse Retained for periods as defined in retention schedule	External NHS **Security Measures**: • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	High risk to pupils as we hold a large amount of personal and sensitive information	

Data Mapping

Purpose	Whose data	What data – Type of Data Source of data Legal basis	When it's collected Who is it shared with & why How long is it retained & why	Where it is stored? *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	Potential Risks	Amount of Data
Photos External Photographer used: Wrates	Pupils	**External Photographer:** Individual and group photos. Photographers are given name, DOB and tutor group to enable photos to be matched for import to MIS. Photos used for: • Distributed to parents/carers for purchasing • School ID badges and display board for staff in entrance foyer **Basis** – Vital interest [safeguarding] and legitimate interest for distributing to parents/carers. Detailed in privacy notice. **Source** – Individual School may take photos of pupils in normal school activities for displays in non-public areas of the school. **Basis** – legitimate interest. Detailed in privacy notice. **Source –** Individual consent Photos taken of pupils during normal school activities for use in public areas of the school, newsletters, prospectus and publicly accessible media i.e. websites **Basis –** Consent from parents/carers for Yr7s and under – Consent from individuals from Yr8 and above. Granular consent to clearly specify where images and names can be used. **Source –** Parents/Carers/Pupils Photoshoots for promotional campaigns **Basis** – Consent gather prior to each campaign **Source –** Parents/carers/pupils	External School Photographer: Photos taken twice a year Photos are used: • Distributed to parents/carers for purchasing • For displays in school • For newsletter/prospectus articles • For the school website • For promotional campaigns. To have/put 3rd Party Data Sharing Agreements in place if applicable Retained in MIS in line with retention schedule.	Stored/Shared with eternal photographers. Staff photos in internal school network & Cloud systems On a CD provided to school Hard copies which may be displayed on school website, marketing literature (prospectus e.g.) and social media **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	Photos taken of pupils who have opted out. Photos used where consent has not been given. Photos included in promotional material without proper consent. Detailed records of consent not kept. Images taken on staff personal devices Images stored on staff personal devices or sent to personal email	Photo taken of all pupils for safeguarding. Varying amount of phots taken for other purposes.

Data Mapping

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Injections Height & Weight Checks (primary)	Pupils	No additional data is collected or processed. We collate consent forms for the NHS vaccination team.	Paper copies of parental permission collected by school and handed over to the NHS To have/put 3rd Party Data Sharing Agreements in place if applicable	External Hosted **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers		

Data Mapping

Purpose	Whose data	What data – Type of Data Source of data Legal basis	When it's collected Who is it shared with & why How long is it retained & why	Where it is stored? *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	Potential Risks	Amount of Data
Workforce Requirements	Staff	Personal Data: Name, DOB, address, contact details [phone and email], employee/teacher number, national insurance number, emergency contact details, next of kin Contract information: start dates, hours worked, post, roles and salary information, bank details, employment history. Work absence information (number of absences, periods of time, reasons – including information regarding physical &/or mental health), holiday records. Qualifications, training courses attended etc. Performance Information (appraisal, performance reviews, improvement plans, disciplinary or grievance records etc.) Other information such as pensions arrangements, application information, reference information Special Category Data: Additional information such as, gender, age, ethnic group, religious or similar beliefs, trade union membership (where permission has been given to pay subscriptions), information about declared medical conditions/disabilities, genetic information and biometric data, data connected to Disclosure & Barring including disqualification by association, CCTV footage & images **Source –** Individual/Line Leader/Senior Leaders/Medical Establishments/Tax & Regulatory Authorities/Previous Employers/Trade Unions/DBS Administrators/Insurance Benefit Administrators/Recruitment or Vetting Agencies/CCTV Systems/Messaging Systems/ Communications Systems, Remote Access Systems, Email and Instant Messaging Systems, Intranet and Internet Facilities, Telephones, Voicemail and Mobile Phone	At the point of application &/or appointment Throughout the year for performance, review, training, attendance, holiday records etc. Application/Appointment or Throughout the year as necessary for declared medical conditions/disabilities, medical/health referrals Throughout the year for photographs/videos/CCTV footage/website/phone & communication systems **Shared with:** Local authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes Nottingham Roman Catholic Diocesan Education Service & Catholic Education Service The Department for Education[and/or the ESFA], in compliance with legal obligations of the school to provide information about our workforce as part of statutory data collections and other Government Department statutory data returns Contractors, such as payroll providers, to enable them to	Staff Files School MIS Systems Performance, Attendance, Holiday, Training Recording Systems Website/CCTV/Phone Systems HR DBS Recording/Logging System Sickness Absence Portal School Budget **Security Measures:** • Password Protection • Permissions on File Systems • Permissions in MIS • Server in locked room • Lockable cupboards/drawers	High risk to staffs as we hold a large amount of personal and sensitive information	Hold data for approx 47 Past data retained in line with retention schedule

Data Mapping

Workforce Requirements (continued)	Staff (continued)	Records, External Payroll Providers, Occupational Health Providers, Local Authorities. **Basis –** Legal Obligations / Required by Contract / Public Interest / Vital Interest / Consent	provide an effective service to the school and government agencies such as HMRC and DWP regarding tax payments and benefits Our professional advisors including legal and HR consultants Pension administrators Student Loan companies (where applicable) To have/put 3rd Party Data Sharing Agreements in place if applicable Retained for periods as defined in retention schedule & CCTV Policy			

Data Mapping

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Governance	Directors, Foundation Governors, Parent Governors	Name, Address, Email Address, Telephone Numbers, Governance Terms of Service, Business Interests, Skills Audit Report information, DBS Numbers, Disclosed Additional Notes/Roles **Source**: Individual/NRCDES/DBS Administrators **Basis –** Legal Obligations / Public Interest / Vital Interest / Consent	During the appointment stage to Directorship or Foundation/Parent Governor Shared with NRCDES and NCC Governor Services for registration/information analysis/recruitment purposes Shared with Chairs/Heads for information analysis/recruitment purposes Throughout the year when personal profiles are updated on Trust Governor System or with the collection/annual completion of Business Interest Declarations For Audit purposes Retained for periods as defined in retention schedule	Trust Governor System HR DBS Recording/Logging System **Security Measures:** • Password Protection • Permissions on File Systems • Server in locked room • Lockable cupboards/drawers	Medium Risk – Confidential but not Sensitive Information Secure individual log-ins per Director/ Governor	Approx 150 records

Data Mapping

Purpose	**Whose data**	**What data – Type of Data** **Source of data** **Legal basis**	**When it's collected** **Who is it shared with & why** **How long is it retained & why**	**Where it is stored?** *Manual, electronic, in-house system, BYOD/remote working, External hosted, Cloud service*	**Potential Risks**	**Amount of Data**
Visitors	All visitors on site during school hours	Name, Car Registration & possible CCTV footage **Source**: Individual & CCTV systems **Basis –** Legal Obligations / Public Interest/task / Vital Interest	Obtained from the individual on the day of the visit. May be captured on site CCTV on day of the visit. For Health & Safety purposes and for Safeguarding purposes. Retained for periods as defined in retention schedule & CCTV Policy	Visitors sign in using a GDPR compliant visitor book. **Security Measures:** • Password Protection • Permissions on File Systems • Server in locked room • Lockable cupboards/drawers	Low Risk – Name & Vehicle registration only	Approx 500 records