Department
for Education

Data protection: a toolkit for schools

Beta version

April 2018

Contents

Summary

About this guidance: status and version control

Version: Beta Date of release: 23 April 2018

This document has been released as a Beta version. This means that we are confident that overall, the document adds value in achieving its aims of supporting schools to better manage data protection and to implement the new elements of data protection associated with the General Data Protection Regulation (GDPR) and associated Data Protection Bill which will replace the current Data Protection Act 1998.

We are also aware that as a first version it needs to be:

- tested by schools for readability and ease of use
- viewed by a wide range of stakeholders who are interested in ensuring that schools deal with data protection robustly and efficiently

Feedback obtained during those processes will help iterate and improve the toolkit.

Hence, alongside the publication of this document, an informal consultation exercise will run until Friday 1 June 2018. The initial feedback gathered will be used to inform a revised version. The document is also likely to be refreshed once the Data Protection Bill is finalised. After that, we anticipate that it will still be a 'living document' and there will be further opportunities for improvement over time.

Whilst the document is currently long, it has been created to include a number of case studies and annexes that the schools who have contributed to the toolkit have found useful. It is intended that schools may choose to read the bits most relevant to their own maturity in managing data protection.

If you wish to comment on the content of this document then please provide feedback to data.modernisation@education.gov.uk with the subject heading "GDPR toolkit feedback". If your comments refer to specific content in the document, please reference the page number(s) to identify the area to which you are referring. Please return comments by Friday 1 June 2018. We may not be able to provide individual responses to feedback, but all feedback will be read, considered, and inform future thinking as appropriate.

Reference materials used within this document

In order to support schools to access supporting materials efficiently, a number of links are provided to materials created by public and commercial bodies, and case studies are provided from a range of volunteer organisations.

Any links to materials produced by commercial organisations are only done so after satisfying the following criteria:

- The material is assessed as being informative and correct.
- The material is assessed as adding value by a panel of school leaders working on data management.
- The commercial organisation that produces it may be referenced within the material, but the material must be free from any sales material or promotional material related to services offered.
- Access to the resource must be freely given without the need to register or provide contact details.

By referencing any open source external material, the Department for Education (DfE) is in no way endorsing or recommending any additional services or solutions provided by third party organisations. Schools are of course free to undertake their own searches for open-source material that helps them fulfil their statutory duties.

As well as those organisations providing information links, a number of other organisations have helped in developing the content of this initial toolkit. They key people and organisations involved are outlined in Annex 10.

If, as an organisation, you have material that you feel would support schools in managing data protection, **and satisfies the above criteria**, please provide details to the consultation email address (data.modernisation@education.gov.uk), with a view to it being considered for inclusion in subsequent versions of this document.

Foreword by Neil McIvor, Chief Data Officer, DfE

Data plays a key part within a modern education system. It provides the opportunity to effectively monitor the progress of learners, it allows evaluation within evidence-based practice, and it provides the opportunities for huge efficiencies in how school life operates.

The use of data across our sector and beyond has developed significantly in recent years. And so it is right that the law, processes and skillsets associated with being effective guardians of children's data are brought up to date and fit for the modern era.

As the new data protection legislation comes into effect in May, it provides a challenge and an opportunity. Understanding and aligning to the changes is a challenge for all organisations, big or small. It does though provide a thorough opportunity to refresh policies and procedures relating to the safe stewardship of data. The new legislation is generating momentum around auditing where organisations are at, identifying risks and developing coherent plans to manage them down. It also places a firm emphasis on citizens being informed on the use of data and their associated rights. If our sector is to be entrusted to hold sensitive data about children across the country and exploit the benefits modern data technologies enable us, then they are both to be welcomed.

In aiming to support schools with the changes, it is clear that there is no one voice or lens in our sector who could have written an excellent guidance document in isolation. That is why I'm delighted to see the high degree of collaboration from schools, local authorities (LAs), multi-academy trusts (MATs), and the supplier community who have helped develop this initial working document.

We would really value your comments and feedback during the informal consultation window, so that we can continue to work with users to iterate and improve it.

Yours,

Neil McIvor, Chief Data Officer, Department for Education

Structure and purpose of the toolkit

Much of the best practice associated with the General Data Protection Regulation (GDPR) and Data Protection Bill is based on the Data Protection Act 1998. That said, GDPR and the Data Protection Bill introduce new elements and provide an opportunity for organisations to review their current data protection and privacy practices.

Schools will be at different stages in preparation for legislative change on data protection. The use of data and related technologies varies significantly across our schools, and this toolkit is intended to support schools in developing the policies and processes that are right for them. It has been developed by the Department for Education (DfE) working in collaboration with schools, multi-academy trusts (MATs), local authorities (LAs), system suppliers, GDPR support providers, the National Cyber Security Centre and the Information Commissioners Office (ICO).

The document provides 9 steps that, we think, can help schools efficiently develop the culture, processes and documentation required to be compliant with the strengthened legislation and effectively manage the risks associated with data management.

The 9 steps outlined a suggested sequence of activities that will enable schools to identify and monitor the use of personal data, undertake the necessary processes for auditing and assessing risk, and assist with compiling policies to ensure schools can sustain compliance. Each step is structured to provide the intended outcomes of each step, a suggested ‘how to’ approach, top tips, case studies, and links to the most relevant resources for that step that have been identified to date.

It is important to note that this document provides tips and guidance only. It is intended to support schools draw out areas of risk. Where the term ‘school’ is used, multi-academy trust could equally apply where relevant, as the legal entity with the responsibility for data protection for their schools. **It does not constitute formal legal guidance**, **and as a data controller in its own right, a school is ultimately responsible for its own data protection procedures and compliance with legislation.**

Step 1: Raising awareness

Intended outcomes:

1. Raise awareness across **all** staff within the school who come into contact with personal data (noting that personal data can relate to pupils, staff, parents and potentially others). Making the link between data protection and child protection can be an effective way to 'make it real' for staff, although data protection is much broader than that.
2. Ensure that a broad range of staff across the school community are engaged with the work, to articulate and demonstrate the totality of personal data owned by the school, and to be engaged in the risk management. This includes an awareness that risks to personal data security can come from online threats like a cyber-attack.
3. Governors and trustees are aware of the key issues arising for the schools from the legislative changes and understand how to effectively monitor and review compliance with the data protection regulations.
4. The language associated with data protection, and the enhanced legislation, is de-mystified.

How to approach this step:

Within a school, there are all sorts of job roles that utilise personal data for a variety of reasons. Some staff will be responsible for ensuring they simply use it responsibly, others will be making significant decisions about what data is used, how it is processed and stored and who it is shared with and how. As such, it is likely that a 'one size fits all' approach to staff training will not work.

From talking with schools, we believe an effective approach is to think about **3 levels of raising awareness:**

1. **All staff** should be aware of what personal data actually is, what 'processing' means in the broadest form and what their duties in handling personal information are. They should be aware of the processes by which they are permitted to use that information, and be **clear of the scope of the permitted usage of that data**. They should be engaged with the **risks around data getting into the wrong hands,** and their responsibilities regarding responding to a **data breach.** The job roles that might warrant this level of training include catering staff, welfare supervisors, library staff, cleaners, first aiders etc.

2. **Those who can influence how data is used, processed and secured.** By this we mean any staff in school who may have the authority to create and store data,

enter data into applications/software or decide if/when they will process certain data. They may also have responsibilities for how paper documents are handled within the school environment. This likely covers all teaching staff as a minimum.

As well as the awareness work, they should have the chance to **review the high-level data maps** suggested in step 2, and be given an opportunity to contribute the different perspective that they offer compared with senior leaders or data leads. They should also be engaged with things like **ensuring there is a legitimate lawful basis and, if relevant, a condition for processing** the information they utilise, and that **storage of data is minimised** to that required to perform the necessary task. They should be engaged in **discussions about identification and mitigation of risks**, and know the governance arrangements that oversees the management of risks**.** In addition, as more schools process and store personal data by electronic means, schools will want to produce user friendly security policies and staff training to help reduce the risk of a data breach. The job roles that warrant this level of training may include, but are not limited to, higher level teaching assistants, teaching staff, office staff, site administrators, information and communications technology (ICT) staff and technical support staff. Everyone can help prevent data loss by following basic cyber security steps.

3. **Senior leaders and executive level, and those who manage the 'data ecosystem'.** By this we mean those in school who are responsible and accountable for making choices around the use of technology and its security, deciding on what and how the data is shared, and setting school policies around the use of data and technology. As well as the senior leadership team (SLT), it may well be network managers or business managers. These people need to be **sufficiently aware of the content of GDPR and the Data Protection Bill, so that they can assure governors that the school has the right things in place to be compliant.** As a data controller the school has a responsibility to ensure there that is accountability, and transparency throughout the whole data ecosystem and that the principles of data minimisation and privacy by design are adhered to by all parties, and that any contracts with data processors cover the relevant areas of data protection. This level of training is aimed at those who are accountable for those responsibilities on a day-to-day basis.
   Job roles warranting this level of training include, but may not be limited to, all SLT members, curriculum leads, business managers, ICT leads and data managers and MAT executive teams.

In addition to staff training, **awareness for governors and MAT trustees** should focus on the following areas:

- That the ultimate responsibility for compliance sits with governors and trustees.

- School governors will also have an oversight role in making sure their school has good network security to keep the personal data they hold protected. This should also include having a business continuity plan in place that has cyber resilience as a consideration.
- That the new legislation moves schools from being required to 'comply' with data protection, to being required to 'demonstrate' compliance with legislation.
- To actively demonstrate compliance, schools need to document all their assets of personal data and ensure they are being appropriately managed and secured.
- Preparation requires a thorough 'audit' or 'housekeeping' exercise on current data processes that should already be in place in relation to the Data Protection Act. In particular, it is likely that data retention policies need more consideration.
- Following the data audit, an assessment of risks to data protection that will be considered by the school to be high or medium should be maintained. Schools should clearly identify what these risks are and how they are being addressed. This could include identifying any shortcomings in the school's network security infrastructure and keeping IT security policies up to date. This should be documented as evidence towards compliance.
- Schools need to review how they communicate their use of data with pupils/parents, and the rights of data subjects, with clear explanations regarding the strengthened rights (including Subject Access Requests (SARs)). Schools need to have agreed procedures for dealing with SARs.
- A need to appoint a Data Protection Officer who has the ear of governors (and vice versa) and is somewhat distanced from the management structure that develops and maintains data policies. (Step 7 has more information).
- A review of data protection policies in light of any changes to procedures and processes arising from the data audit and risk management.
- Reviewing data protection is an ongoing process requiring the whole school to be continually mindful of their responsibilities. Formally scheduling an annual review of current practice through an internal or external audit may be something schools wish to consider.

Top tips:

- Link data protection to child protection when trying to get people engaged. In this way, all staff see that data protection matters in the context of pupil welfare. But the rights of individuals are also key and start people thinking about gaps in current practice.
- Once SLT have developed a high-level data map (as described in step 2), test and iterate it during training with staff. They will identify new things and it will help entrench a sense of ownership.

Case studies

- In training it may be useful to use ‘real life’ case studies to explore how your school ensures that its personal data is safe. “School CCTV hacked” or “Children’s Services Data Breach” are 2 search terms that might find articles that provide food for thought and help make training/risk management feel real.

Relevant resources:

- Annex 1 explains the key terms and language used to describe data protection and within this document.
- There are several posts on the DfE teaching blog related to GDPR.
- An introductory GDPR video on the DfE YouTube Channel.
- This 2m 30 second video by GDPR in Schools (GDPRiS) can help to set the scene as part of training with staff. A print out summary is also available on their website.
- The National Cyber Security Centre website has guidance in this area and will publishing more advice covering the topics discussed above in the coming months.

Step 2: Creating a high level data map

Intended outcomes:

1. Build up an overview of all the places personal data are stored and used in the school (your school's "data ecosystem").
2. Create something that can be discussed and tested with staff to identify any gaps in the initial 'overview' and build confidence that everything is captured.
3. Create an overview that can be aligned to more detailed documentation about data assets.
4. Create a picture that helps communicate personal data use with pupils/parents, a requirement of the new legislation discussed in step 8.

How to approach this step:

One approach many schools are taking is to begin with a session to complete these 3 columns of a table:

1. Data sent to the school from someone else (for example, a local authority admissions team).
2. Data created within the school.
3. Data passed on from the school to someone else (a subsequent school for a pupil, the local authority, DfE or a supplier).

Consider the types of personal data your school records and uses. The data can be categorised as follows:

- admissions
- core management information systems (MIS)
- any 'data integrator software' you may use to connect your MIS with other systems
- curriculum tools
- payment systems
- virtual learning environments
- catering management, including cashless catering
- safeguarding, potentially including CCTV
- trips and transport
- uniform, equipment and photographs
- identity management systems (potentially using biometrics/fingerprinting)
- contract/communication systems
- social care and health interactions (for example, school nurse visits)
- statutory returns
- references and education settings you pass children on to
- workforce systems – such as job applications, current staff and former employees
- paper records
- other systems

A simple way to capture this information is by creating a table with the data types forming the row headings and the data flow considerations forming the column headings. An example is provided in Annex 2.1

Once you think you have captured all the data sets in use within the table, convert the table into a visual map of the data systems, and how the data flows into and out of the school. A visual map is engaging and user friendly, and will be useful in subsequent steps.

Top tips:

- Remember, the focus is **personal** data, that is information that identifies a living individual. Whilst you may want to do this for other data assets as well (for example, financial data assets) the priority is personal data in terms of responding to the new legislation.

- Invite a range of staff to document the data systems and stores associated with each data area. SLT or data managers might initiate the work, but it will be other teachers and school members who spot the gaps and will often have a more comprehensive understanding of paper records or use of learning applications that may not be on SLTs radar.

- Do you have 'middleware'/'data integrators' that extract data from your MIS to be used in other systems? Examples are Groupcall Xporter, Wonde, OvernetData, SalamanderSoft, Assembly/Ark UK group and Ruler. **If so, it is vitally important that you are aware of what information is being extracted from your MIS and how it is being used and/or shared with other systems.** If you don't know whether you use them or not, ask your MIS Provider. **It is critical that the school assesses how its liability may be affected by the actions of your third party suppliers and to mitigate risk it is important to exercise due diligence and ensure you have an up to date data processing agreement in place with them.**

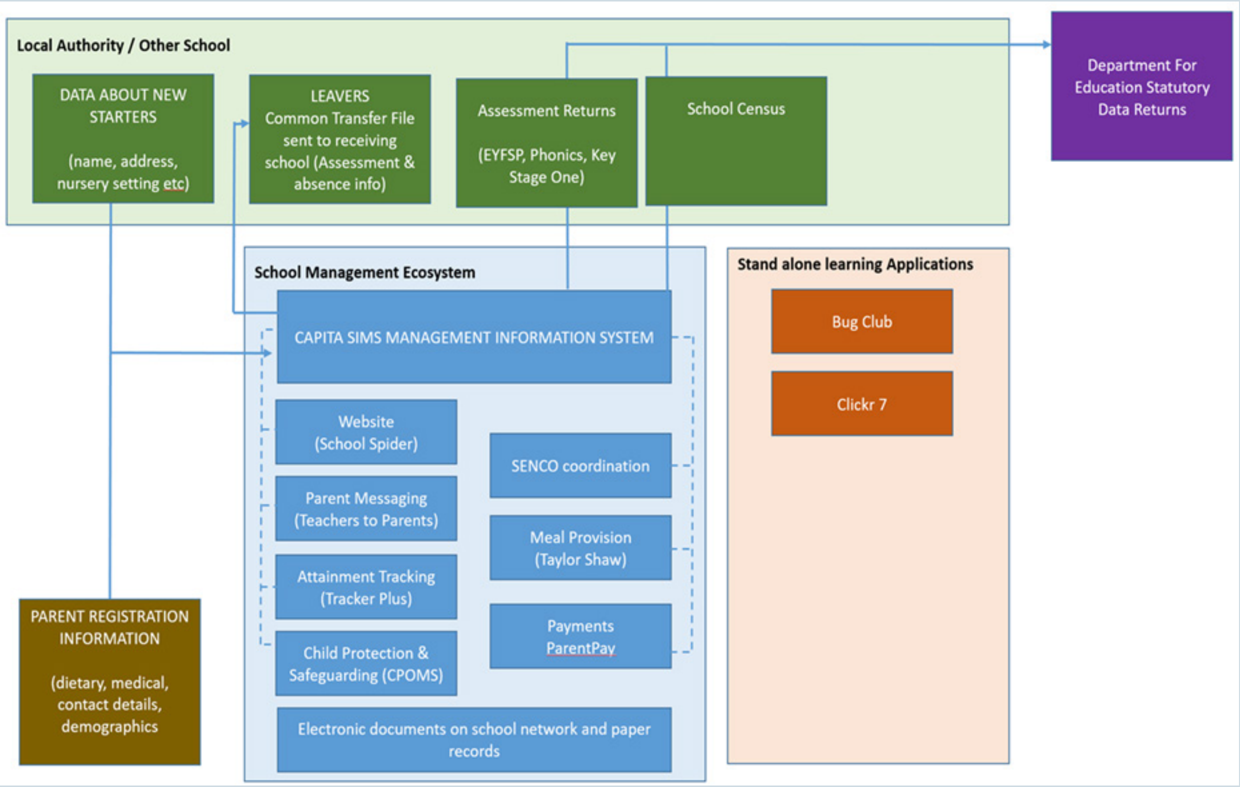
- At this stage it would be a good opportunity to take stock of the IT security policies that your staff currently follow both when you are sharing and storing personal data over networks.

- The data map you create is your 'as is' data map and will help you understand the range of personal data your school uses, how it is used and who it is shared with. **It does not mean that it is compliant with new legislation.** The work you will do in subsequent steps will build on this knowledge to pinpoint areas of weaknesses or potential issues with current practice that need to change.

Case study: Dobcroft Infant School, Sheffield: Pupil data

Dobcroft Infant School undertook a data mapping exercise at the outset of preparing for the new legislation.

Sharing it with teachers and staff proved extremely valuable in validating the map, identifying gaps, and being alive to issues with paper records.


Local Authority / Other School
DATA ABOUT NEW STARTERS (name, address, nursery setting etc)
LEAVERS Common Transfer File sent to receiving school (Assessment & absence info)
Assessment Returns (EYFSP, Phonics, Key Stage One)
School Census
Department For Education Statutory Data Returns
School Management Ecosystem
CAPITA SIMS MANAGEMENT INFORMATION SYSTEM
Website (School Spider)
Parent Messaging (Teachers to Parents)
Attainment Tracking (Tracker Plus)
Child Protection & Safeguarding (CPOMS)
SENCO coordination
Meal Provision (Taylor Shaw)
Payments ParentPay
Electronic documents on school network and paper records
Stand alone learning Applications
Bug Club
Clickr 7
PARENT REGISTRATION INFORMATION (dietary, medical, contact details, demographics

Relevant resources:

- Annex 2.1 includes an example of a table that can be used to support the work to capture all personal level data assets.

- This video by GDPR in Schools (GDPRiS) can be used to help set the scene and context of those setting out on the data mapping and data asset register work with a school. This is also available as a mind map.

Step 3: Turn your data map into a data asset register

Intended outcomes:

1. Create the main framework around which schools can document the detail associated with each dataset.
2. Identify the areas of weakness/risk or gaps that will most likely begin the creation of a risk-management based approach to compliance.

How to approach this step:

- The creation of data map is a useful starting point, but you need to start building up a rich picture of understanding about your data assets. You need to create a data asset register.
- In simple terms, a data asset register is a long list of all the different data assets you have in your school, with some supplementary information about each of them. Different organisations will go down to different levels of detail here depending on their complexity and maturity. As a minimum, doing this for all assets that hold personal level data is required.
- A data asset is a ‘thing’ that contains data. It could be a database, a system used, a spreadsheet, or a set of paper records. It is worth taking time getting the level of detail right here. If you think of your school as a library, then data assets are the books. They are not the most detailed level of data you hold (that would be the words, sentences and chapters in those books), but rather they are distinct portions of your data estate that can be thought of as ‘one asset’.

Your data map will contain a pictorial representation of your data assets. We recommend that at this stage:

1. You give each ‘data asset’ on your data map a reference number.
2. You create a row in a spreadsheet for each data asset you assigned a reference number.
3. You create the following column headings:

Theme	Column heading
Source	• Source of data
Contents	• Does it contain Personal Level Data (Y/N)? • Does it contain GDPR Special Category Data, or other data considered sensitive in education (Y/N?)
Processing and role of the school	• Is the school a data controller or data processor? • If a controller, are there any joint controller relationships? • What processing is done with the data – what is this data asset used for in school? • What is the lawful basis (personal data) and condition for processing (special categories) that apply to that processing?
Controlling access and use	• Is there any onward sharing? To whom? • Is there an up to date data sharing agreement in place? • Who has access to this data asset in school, and how do we control that to ensure only those with permission can see/use it? • When using IT networks is it possible to limit the number of users and grant the least amount of privilege required and monitor their activity?
Data retention and destruction	• What is the data retention period(s) for the different data in the data asset, and what is the justification for it? • Is the capability to manage retention (that is, to delete records or anonymise them after X years) built into software? • If no, what operational process is in place to ensure the intended retention period is implemented properly?
Communicating with data subjects and their rights	• Do you rely on seeking active informed consent, and if so how is this managed? • How are data subjects informed of their rights regarding access? • How are data subjects informed of their rights regarding rectification of data? • How are data subjects informed of their rights regarding erasure of data? • How are data subjects informed of their rights regarding restricting certain types of data processing? • How are data subjects informed of their rights regarding objecting to certain types of data processing? • Is the process for Subject Access Requests, including getting data in a structured format known?

Theme	Column heading
Security and Breach	• What security measures are in place for inappropriate access or loss of a data asset? • Has the school put in place up-to-date ICT security policies to prevent or deter personal data loss for incidents such as a cyber-attack, and do you review it within a defined period? • As part your IT security policy do you follow processes to secure the transfer of data between users and controllers? • Is there a process in place for handling a breach of a data asset including reporting it to the relevant authorities?
Automated Profiling	• Does the processing of the data involve any automated decision making, including profiling?
Offshore storage	• Is the data stored offshore? If so, where?

Top tips:

- Some of this information (where data is stored, the security measures and confirmation that there is no onward sharing) may be required via conversations with your suppliers. DfE has published an open letter to encourage suppliers to support you with this task. Feel free to quote it to your supplier if you are experiencing resistance.

- Ensure that your 'data map', created in step 2, and the data asset register remain in sync at all times. Use versioning control to ensure that they do, that way your data map can continue to be the easy way of visualising your data estate, and the data asset register can be the more detailed management tool, but you can use both with confidence so long as they are aligned.

- Spending a bit of time structuring your data asset register based on logical areas (for example, learning platforms, payment systems) will pay dividends in the long run in terms of 'staying organised' as you build things up, as you change systems over time and will help when putting together a risk register to assess the cyber security readiness of your school. Another benefit is that an inventory of all your systems, and network enabled electronic devices, can help improve your data security further down the line. For example, once you have identified all your systems and devices you can set up policies to keep them properly maintained by regularly updating and patching with the latest security updates.

- Depending on the size of your school, it may be important to develop a classification for your numbering. For example, A = Admissions data, B = Catering systems, C = Communication systems, and then you can develop your list with some structure:

  A. Admissions Data:
  A.001 – Admissions File from LA
  A.002 – Admissions data from Feeder Schools

  B. Catering Systems:
  B.001 – Pupil ordering system
  B.002 – Payment System
  B.003 – Identification System

  C. Communication Systems:
  C.001 – Text messaging system to parents
  C.002 – Email distribution list of alumni / ex pupils

Relevant resources:

- DfE has published an open letter to encourage suppliers to support you with this task. Feel free to quote it if you feel you need greater input from suppliers to help you complete your asset register in relation to system security, onward data sharing and any offshoring of data in particular.

- The Edugeek website is a popular place for data managers and technical colleagues grappling with data protection issues to collaborate and discuss issues associated with information management and data handling.

- The National Cyber Security Centre has published guidance that can help prevent personal data loss due to a cyber-attack. The principles contained in this guide can also help improve your school's cyber resilience from online threats.

Step 4: Documenting the reasons for processing data

Intended outcomes:

1. Become familiar with the conditions and lawful basis for processing that are most relevant to the activity of schools.
2. Understand the extra reasoning that is required to process special categories of data, which are tightly defined in the new legislation.
3. Understand that lawful bases are specific to processing data – that is, the purpose you are using it for.
4. Identify the areas that do not appear to be essential to undertake the task of safely and efficiently running as school, as these are the areas that informed specific consent from data subjects may need to be sought if not already obtained.

How to approach this step:

- Before setting out the legal reasons for processing data, it is important to classify the data in the asset as items with differing sensitivity require different processing conditions.
- Remember that personal data is all the data that relates to an identified or identifiable living individual. GDPR identifies 2 types of personal data:

  Special Category Personal Data – Some items of information about people are highly sensitive. GDPR specifically defines them as data relating to:
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade-union membership
  - health or sex life

  Data relating to criminal offences is also afforded similar special protection.

  Personal data – All other data items related to an individual are merely termed ‘personal data’. These are data items such as an attendance mark, an email address, or an examination result.

Understanding legal definitions can be quite complicated, (they are set out in full in Annex 4.1), but in all probability, the use of pupil data in a school that does not need consent from data subjects falls into two or three main areas provided for in law (workforce data may also be reliant upon being “necessary for a contract”).

Focussing on these, with help from the ‘top tips’ at the end of this section, should help you move through this step relatively quickly.

The first question to ask yourself is:
“Am I required by law to process this data?”
DfE data returns, such as school census and certain responsibilities to return data to the local authority, means you have a **legal obligation** as your legal basis (see Annex 4.1) and your condition for processing the special category data within that is **processing is necessary for reasons of substantial public interest**. This is to comply with GDPR Articles 6 and 9 and the Data Protection Bill (NB: not yet finalised at time of creating this version of the toolkit).

If the answer to that first question is ‘no’, then the second question to ask is:
“Do I need to process this data in order to safely and effectively run my school?”
If the answer to that is yes, then the lawful basis of **public task** may well apply, and again, the **public interest condition may well apply where the data items are special category data.** An appropriate condition from articles 6 and 9 of the GDPR need to be identified. **Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding.** Information that could be relevant to keeping a child safe should be shared so that informed decisions can be made about a child’s welfare.

The next area to explore thoroughly is the data processing that does not appear to be legally essential, nor needed to run your school safely and effectively. These are the areas where other conditions, particularly specific consent of the data subject, may need to apply. Article 4(11) of the GDPR defines consent as:

“…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

Examples here from school life might include:

A. A school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.

B. “Marketing” materials to pupils/parents. This might include ‘non-school’ material, for example, if a local holiday club pays you to email parents with details of the holiday club, that is not an essential part of running the school. Or it may include school material such as fundraising campaigns. Consent will definitely be required if such communications are carried out electronically, because of the Privacy and Electronic Communications Regulations (PECR) but if marketing is paper based, the lawful basis of legitimate interests could possibly be considered, subject to the usual balancing tests.

C. Maintaining databases of former pupils contact details long after they have left for fundraising or other purposes requires consent and a retention policy.

Importantly, if relying on consent:

1. Consent must be voluntarily given; it must be specific, informed and unambiguous, and able to be refused with an alternative process on offer. People should know exactly what they are signing up to.
2. Individuals must be able to revoke consent at any point and procedures need to be in place to allow individuals to withdraw consent.

Top tips:

- It is important to capture the legal basis/conditions for processing. It determines the answer to 'what am I allowed to process?'
  On its own, justification for processing does not provide compliance. Just as important as the 'what?' is the, 'how do I process it responsibly?' So, whilst a legal basis exists for processing that a child is looked after, a school also needs to consider: how many people have access to which data, do they really need that level of access, what degree of history is necessary, how the security of the data is handled as a result of system security and policies how that data is used within the school. The school should also check that they are being transparent with data subjects about this processing.

- Within education, we do process some sensitive information about children that is not set out in the legislation as a 'special category personal data'. Notably information about children's services interactions, free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information and some behaviour data. **We consider it best practice that when considering security and business processes about such data, that they are also treated with the same 'high status' as the special categories set out in** law.

- **Remember that the reasons/conditions relate to the processing activity, not the data itself.** For example, the processing of a parent's phone details might be 'to text message urgent school information, and contact in case of an emergency relating to their child'. That is essential to run your school well as a public task. That does not justify passing their phone number on to someone who wants to market tutoring services in the local area. Conditions for processing should cover the data items within an area, the purpose, the people, and ensure that necessity and proportionality are considered at all times.

- If you are relying on legal obligations as your condition for processing, think about what happens after you have fulfilled that legal obligation. For example, if you want to retain gender data on year 6 students after the summer school census, and the legal obligation is no longer relevant as the data has been sent to DfE, you need another lawful basis to rely in of you are to retain and use that data.

- Consent should not be relied upon for processing essential for a school performing public tasks and for data in a learner's Education Record. For example, you **do not** need parental consent to enter children for exams. If you are relying on consent, it must be easy to give and to withdraw. It should be voluntarily given without feeling forced to agree. If a data subject feels that they 'must' agree, or saying no is unduly awkward, then this is not a genuine consent process and a different legal basis should be used.

- Article 7(2) of GDPR addresses pre-formulated written declarations of consent which also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32.39

- Explicit consent should always be used for biometric data usage (and for that purpose only) – and if any one of the pupil or parent/carers do not wish to give consent, a genuine alternative must be offered. For example, stating "you can bring in a packed lunch" is not a reasonable alternative to a data subject not wishing to provide biometric data to support catering management. A pin number would be. This is set out in the Protection of Freedoms Act.

- You may find that more than one condition for processing applies. If so, it is good practice to document all that apply at this stage.

- **Safeguarding**: GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.

Case study: Ensuring data subjects have their rights respected when using biometric data – model policy provided by the Oxford Diocesan Trust (sourced from 'The Key, in partnership with Forbes Solicitors and Emma Swann)

If and where the school uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act, 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will seek written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school's biometric system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time and the school will delete any relevant data already captured.

Case study: Appropriate use of photography

Photographs are used in school for many different reasons. The different uses should be considered separately and potentially have different conditions for processing. For example:

- Photographs used in identity management may be essential for performing the public task of the school, but should to be deleted once a child is no longer in that setting, as it is no longer needed for the purpose for which it was held.

- Photographs in the school environment relative to providing education may fall under the public task purposes, but after the child has left the school this argument becomes weak and may not be lawful; permission to retain beyond their time in school (if required) should be sought. For example, if the child is in a display showing a scientific experiment being done that you wish to retain as a learning resource for future years.

- Photographs used in promotion/marketing type material should seek specific informed consent, and only be used in line with the consent provided.

Relevant resources:

- The Information Commissioners Office (ICO) website provides more details about the lawful basis for processing, and for special category data, the conditions for processing. These are also provided in Annex 4.1.

- This short video by GDPR in schools provides a 3 minute commentary on the lawful basis relevant to schools.

Step 5: Documenting how long you need to retain information

Intended outcomes:

1. Create a workable data retention policy that can be discussed and iterated with those who best understand your uses of data.
2. Understand that data retention is based on justification – if you can justify it, you can keep it.

How to approach this step:

- Schools need to be mindful that at present there isn't a 'sector wide data retention policy' guidance document. Annex 5.1 is a very first iteration, but if one is to evolve it will take greater engagement and consultation than has happened to date.

- It is important to understand that you cannot easily think about data retention at the most detailed level of individual data items – it is the context they are being applied that is relevant.

- Data retention does not have to be 'all or nothing' – as data becomes older, there are steps that schools can take to retain the power of pupil level data for analytical purposes, without the need to keep detail such as name and full address.

- The requirements for data retention as set out through legislation has not significantly changed through GDPR and examples of best practice already exist (for example, the IRMS Schools Toolkit), but many other aspects of data retention have changed due to how and why data is processed under GDPR and increased emphasis on data minimisation.

Before tackling this, ensure you are comfortable with some of the simple terminology introduced in Annex 1:

Term	Description	Example
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data item	A single piece of information about a data subject.	“Ethnicity = white British” “Attendance = 97%”
Data item group/element	A group of data items that are typically captured about the same activity or business process in school.	Behaviour management or catering.
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay, MyMaths.
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.

These terms are important as we start to think about how long data is kept for. The focus should be on the time period that is ‘necessary and proportionate’.

Data items are extremely detailed, and to think them through it helps to group them together into data item groups. Similarly, with over 1,000 systems in use in the education sector, grouping into overarching themes can help provide focus.

When working with a group of people from schools, LAs, MATs and suppliers, we found grouping data items about pupils into the following areas was the most workable set of data item groups:

- admissions
- attainment
- attendance
- behaviour
- exclusions
- personal identifiers, contacts and pupil characteristics
- identity management/authentication
- catering and free school meal management
- trips and activities
- medical information and administration
- safeguarding and special educational needs

We used the Common Basic Dataset as the starter for creating the scope of what a school initially needs to focus on.

Once you have your list of data item groups, think about 4 periods of data retention:

1. One month after the event about which you create data is active, in order to ensure any ‘loose ends’ are tied up.

2. One year after the pupil to whom the data relates is at your school, in order to ensure smooth ‘handover’ activity related to the child is passed on to a subsequent school.

3. For 5 years after a pupil has left your school, to support longer term but detailed analysis of progress, attainment, support for different pupil groups etc. This is the area where ‘blurring’ of the data discussed below can gain most traction.

4. Long term, until the child is 25 years of age or older, for instances where detailed information about activities in school may form an important part of safeguarding for that individual.

When setting a data retention policy, consider the following questions:

- Why am I holding this data?
- Do I need to pass it on? Once I have passed it on, am I required to keep it? Do I still need to use it?
- What is the school’s actual responsibility – is appropriate long term retention actually someone else’s job such as a receiving institution or local authority?
- What might Ofsted expect from me in terms of the length of time I can perform detailed reporting?
- As time goes on, can I delete some of the information – for example would aggregated data (‘counts’ of pupils that you might share with governors) or de-personalised data (individual rows, but with names and other identifiers removed) do the job just as well?
- “Because I always have done” is not a justification, but it may be a clue as to a justification. “Why might we have that policy?” Is a good question to ask.

A number of schools have collaborated with sharing thinking on data retention with us in creating this document, and their shared work is provided in Annex 5.1. This is provided to stimulate thinking and discussion at a local level. As data controllers, schools should determine their own policies that work for them and their particular context.

A way to reduce sensitivity over time

When discussing data retention with colleagues across the sector, a common theme emerges. At some point in the pupil lifecycle, detailed fully named and personally identifiable data is needed. Before being comfortable deleting that data completely, there is usually a period where names or full addresses may not be needed, but individual level data still is. After that, there may well be a period where aggregated or summary statistics are all that is needed, and that retaining these for a long time was a good idea.

As we move through time and data becomes older (e.g. the years after a child leaves the school), schools may be able to take steps to remove some of the risks around personal level data by de-personalising it. That is, by taking the names and personal identifiers away, but retaining the data at individual level, schools can still undertake the longer-term analysis of trends or studying of impact on small pupil groups, but the underlying data being retained carries less risk than keeping all the personal identifiers within the data of interest.

This concept is hard to communicate, and to do so people increasingly talk about the 'blurring of a photograph'.

With pupil names and other identifiers, the data is instantly personal.	Typically, once the pupil has left, we need to ask if we still need identifiers like name or data of birth. Could 'term of birth do'? If so, that is good practice as it 'blurs' the data slightly.	Over time, can we retain aggregated summary statistics that are highly blurred? For example, the sort of data that might be shared with all governors.

This is an important concept; GDPR requires data minimisation and data protection by design and default (Article 25) – meaning data controllers and processors must implement appropriate technical and organisational measures, such as this 'blurring technique' (pseudonymisation), which are designed **to implement data-protection principles, such as data minimisation.** These techniques reduce risk, but do not negate the need for compliance with legislation.

Top tips:

- You can’t think about data retention/deletion at the data item or data item group level only. A good data retention policy needs to look at how long you retain data items within the different areas of administration of school life. “How long do we need to keep pupil names in our catering system?” and “how long do we need to keep pupil names in our safeguarding system?” are better questions, and may well generate different answers.

- We learned from discussion that within some areas of data, there is inconsistency in local practice in terms of data retention periods requested of schools, notably around safeguarding data. Follow your local best practice so long as it remains justifiable.

Relevant resources:

- In March 2018, DfE joined a number of schools, MATs, LA representatives and system suppliers to have a ‘hack day’ thinking about data retention. The combined data retention policy for a school from that thinking is set out in Annex 5.1.
- DfE is aware that several schools make reference to the IRMS Toolkit when setting data retention periods. The IRMS is a not for profit organisation that supports the Information and Records Management Profession. As part of their current model they make some content available as open source.

Step 6: Reassurance and risks

Intended outcomes:

1. Identify risks which emerge from the initial completion of your data asset register.
2. Assess what can be done to eliminate or reduce areas of medium/high risk and set action plans to do so.
3. Use Data Protection Impact Assessments as a part of your risk identification and mitigation procedures.

How to approach this step:

- A logical place to start identifying issues and risks is the data asset register outlined in step 3. This will likely identify high-level issues. The most important things to look out for include:

    - Any “current activity” which does not map to a lawful basis and conditions for processing.
    - Do you have uncertainty about onward sharing? As a way to test this, could you demonstrate to a pupil which piece(s) of their personal data have been shared with whom, and when? If systems are moving data, they should be able to report on it. Do you think that you will be less likely to carry out safeguarding activities? If this is the case, it would be useful to re-assess how you are applying the law in this context.
    - Do you have an up to date data sharing agreement with organisations you are passing data on to?
    - Are your IT security policies up to date and is everyone handling personal data aware of your security policies and appropriately trained?
    - Do your systems allow you to implement **your** data retention policy? If not, then it is the system that should adapt to meet your needs, not your data retention policies being compromised to meet any limitations of a system.
    - Do people in your school know what the process is for reacting to a data breach? Have the processes (including IT response and recovery plans) for reacting been tested? Ensure sufficient time is given to the “here’s how we assess impact and minimise that impact” in your data protection policies.

- The data asset register does not flush out all risks and issues. However, regular reviews, use of external experts/advisors, and the involvement of the Data Protection Officer and data protection lead will all help here, as will the completion of Data Protection Impact Assessments.

- A Data Protection Impact Assessment (DPIA) is a tool to help you identify and minimise data protection risks. Conducting a DPIA meets, in parts, an organisation's accountability obligations under GDPR, and is an integral part of the 'data protection by default and by design' approach. An effective DPIA helps you to identify and fix problems at an early stage, demonstrate compliance with your data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage, which might otherwise occur. In some cases GDPR says you must carry out a DPIA, but they can be a useful tool in other cases too.

Top tips:

- **Minimisation** is a key thing to think about:
  - Think about the minimum amount **of personal data** that is needed to get the job done. If an external consultant is coming in to look at progress of pupils in primary schools, then if month of birth or term of birth would do the job, there's no justification for passing on date of birth.
  - Think also about the **minimum amount of people that need access to personal data.** People should only see the personal data they need to see to perform their role. If the number of people seeing the data is indefinite, then this should be made explicit to the data subject.

- Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA). A DPIA is a process designed to describe the data processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance. A DPIA is required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). Examples of when you need to conduct a DPIA:
  - **Data concerning vulnerable data subjects** Vulnerable data subjects include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection
  - **Innovative use or applying new technological or organisational solutions,** like combining use of finger print and face recognition for improved physical access control, Certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.
  - **CCTV**

- DPIAs will need to be frequently reviewed and kept updated. For example, the activity which is subject to the DPIA may slightly change and present new risks as a result. Your school will also need to review all uses of personal data on a regular basis to check whether any activity has started to present high risks to individuals and therefore requires a DPIA.
- Many data breaches occur via ‘innocent mistakes’/human error, and unintended misuse of technology. Ocean Learning Trust are one trust that has withdrawn use of memory sticks/flash drives completely as part of their process to mitigate risk. If you decide to use removable hardware containing personal data you should think about, and limit, who has access to removable media. You should scan all media before importing onto the corporate system and employ encryption, strong passwords and other means of protection.
- Unfortunately, data breaches also happen because of targeted actions by malicious actors and hackers who can be based both internally or externally to the school setting. Regularly reviewing your IT security policies and processes are a must and simple steps like: Regularly updating your software; Employing strong passwords; Using anti-virus software, using encryption, protecting external devices and not leaving your computers unlocked can all make a real difference in preventing IT based data breaches. Staff awareness training on data gathering techniques used by cyber attackers can also be of benefit.

The following case studies focus on some known areas of risk common to many schools.

Case study: Pupils and medical information

Many schools have pupil photographs and key medical conditions on the staff wall. At the onset of thinking about GDPR, one school was thinking, “We ask parents for consent, but that’s special category personal data, should we take it down?”

When thinking it through the school decided:

- Consent was actually the wrong basis for processing. Although well intentioned, the information is actually deemed essential for keeping certain children safe. As such, it’s part of fulfilling a public task, consent should not be used. But at the same time…
- Checks could be done to ensure that it was only relevant medical information (that is, that which a member of staff needed to know in order to keep the child safe) that was used in this way.
- Further steps could be taken to minimise the amount of people who could see that information by re-positioning it and ensuring that only the right people had access to that room – that the space is ‘well policed’.
- That, as part of ensuring parents are informed, whilst consent is not sought, a clear statement about what is held, why it is important for keeping the children safe, and what steps there are to look after that special category data was good practice.

Case study: Mark books and target setting – two ends of the digital spectrum, but both with risks to manage

The data map done in step 2 will likely show a very diverse ecosystem. Most primary schools for example have many paper documents, including pupil workbooks and mark books. These are often very ‘visible’ in classrooms. Whilst some personal information will be needed within them, practices which appear to unnecessarily increase the amount of sensitive pupil data, such as pupil premium and looked after status being contained within them should be avoided.

At the other end of the spectrum, many schools use software packages to support pupil target setting and progress reporting. If this is done ‘blindly’, with software generating targets that go on to trigger various interventions depending upon that target, then it is arguable in the automated profiling territory, outlined in step 3. Ensuring staff see the inputs, can check the outputs to ensure errors in processing are picked up, and can manually adjust targets where other factors not contained within the progressing algorithm are relevant, would all seem good steps to take.

Case study: Taking personal data home

“Can we take information home about pupils?” is a common question raised. This applies to both previous/current legislation and new legislation. An organisation must be clear on:

- What information? – Like many areas of data risk management, has the boundary about what is necessary to perform the required tasks been established?
- What devices and software? – Have you ensured they are secure when being worked on outside the school environment? Has the policy on working on own devices (if allowed at all) been refreshed and reviewed?
- What training/awareness? – Are you confident that people using the information have the right level of training to be alive to all of the different risks that may present if using personal data outside of the school environment? Staff should be very aware of the breach notification process and how to trigger this if working remotely.

If having done that sort of thinking, an organisation feels confident that the risks around personal data are being well managed even when used remotely, then the law does not prevent it from happening. It is for the organisation to assess the benefits of working in this way, and that risks are being appropriately mitigated.

Case study: Using IT intelligently to reduce risk: Queen Elizabeth's High School, Gainsborough

One of the risks Queen Elizabeth High School (QEHS), Gainsborough identified early was the potential for any member of staff generating ad-hoc reports in the management information system (MIS) downloading the data onto an unsecure memory stick or personal laptop. It is incredibly useful for staff to be able to download lists of student names, other personal data or exam scores in order to be able to manipulate the data to provide insights into the achievement of groups of students and thereby set the best learning activities for them. However, there was a high risk of data breach if the memory stick or laptop was lost and the data was not encrypted.

Their solution has several layers of security to it in order to control the risks, but without placing an undue administrative burden on the staff of the school. They have provided every member of staff with a memory stick encrypted using a free to use encryption tool. Each memory stick is assigned to a member of staff and logged. No other devices can be used to download files from any computer in the school. Within their GDPR policy and staff behaviour code they have made it clear that no other memory source is to be used and if the data is taken off-site it is not to be loaded onto unencrypted computers at home.

If a member of staff wants a particular data set they email a member of the office staff who has received training indicating what data they want, why they want it and for how long they will keep the data. All of this information is logged so that the school has a record of all data exports that have been undertaken.

The data is then extracted as a spreadsheet, zipped, password protected and placed in a secure area of the school network for a limited time in order for the member of staff to collect it. The password is emailed to the member of staff separately.

As a result, QEHS Gainsborough are confident we have controlled the risks sufficiently to allow staff to continue to use this data as they did before in order to enhance our support for the students whilst protecting the data sufficiently to meet the requirements of the GDPR.

Case study: Reducing the risks associated with hardware: Broadmead Lower School, Bedfordshire

Broadmead Lower was thinking about the information risks associated with their printing and photocopying, which uses rented hardware. All classrooms and the office staff are networked into one printer, which is very cost effective. However, GDPR prompted some fresh consideration of risks.

- **Internal breach risks** existed because others could access printing before the intended recipient collected it, particularly when printers jammed and the print completed the intended job subsequently. This was significantly reduced by each staff member having a code that is used to run jobs when they are there to collect them, rather than as soon as they click print.

- **External breach risks** the preparation for GDPR meant the school felt more informed to ask about the hard drive in the machines: what information is retained? How long for, why and who can access it? What do the rental company do with that data once the machine is taken away? What evidence should we seek to confirm data destruction? What other networking and remote access risks do we need to consider?

Head teacher Kim Hewlett reflects:
“We decided to formally ask these questions when selecting a new supplier. I worked with our IT support providers to ensure that the information we got back was plain English and understandable, and as a result we are confident we now have the best solution for mitigating risks associated with printing and photocopying in our busy school”.

Relevant resources:

- To ensure Data Sharing Agreements reflect best practice, it is worth looking at the ICO Data Sharing Code of Practice. This includes a model data sharing agreement.
- Information about GDPR compliant contracts can be found on the ICO website.
- Although written about the Data Protection Act 1998, the ICOs ‘Bring Your Own Device’ guidance covers many of the risks and practical steps for schools to take when weighing up remote working of staff.
- GDPRiS has a useful document about the things schools will want to know from suppliers in order to demonstrate GDPR compliance.
- Annex 6.1 contains a Data Protection Impact Assessment template provided by CBICT, an organisation that supports schools in central Bedfordshire.

- The ICO website contains good information about when and how to best conduct Data Protection Impact Assessments as part of identifying potential areas of risk.
- The National Cyber Security Centre has a range of guidance on its website which can help keep your systems and personal data secure from online threats.
- The European Commission has guidelines on personal data breach notification

Step 7: Decide on your Data Protection Officer role

Intended outcomes:

1. Understand the role of the Data Protection Officer (DPO), and be clear that each school needs to appoint a named DPO in order to be comply with new legislation (note, this DPO can be named as a DPO for more than one school/organisation).
2. Understand the different options for a school appointing a DPO, so that schools can consider the best value and appropriate method for them.

How to approach this step:

The first step is to understand the responsibilities of the DPO, and the greater degree of separation between the DPO role and the 'data ecosystem manager' than has previously been the case under the Data Protection Act 1998.

Responsibilities of the Data Protection Officer

Currently, schools have leads on data protection but very often they either are, or work very closely with, the person who has established the ecosystem. The new legislation encourages a degree of separation between those in charge of the ecosystem, and the DPO role. The DPO needs to be:

- **Highly knowledgeable** about data protection, GDPR, the schools operations, technology and security
- Well placed to promote a **data protection culture** within a school

The DPO role involves advising school leadership and staff about their data obligations, monitoring compliance, including managing internal data protection activities, training, and conducting internal audits.

The DPO will also need to advise on when data protection impact assessments are required, and be available for data protection enquiries from parents and pupils. Additionally, they need to be able to report directly to the board and be the point of contact for communication with the Information Commissioner.

Options for appointing a Data Protection Officer

The second step is the need to consider the pros and cons of the different options for appointing a DPO. There appear to be 4 options available to schools:

1. **Re-align responsibilities within your current team** – create the DPO role within your team that is sufficiently removed from those making technology or processing decisions.

2. **Collaborate** – share the DPO function between a group of schools, or share expertise by being the DPOs for each other's school.
3. **Contract** – it is possible to buy in the DPO function for your school or group of schools.
4. **Seek volunteers from experts that may exist in the wider school community**. This might be possible, but note that as a volunteer their statutory responsibilities remain at the same expectation as a paid DPO. It would be a reasonably big commitment for that volunteer, and they would need to be able to clearly convey risks and views to senior managers.

Effective working with a Data Protection Officer (DPO)

The DPO should be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and schools should seek the advice of the DPO when carrying out impact assessments. Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the school's data governance. In addition, it is important that the DPO be seen as a discussion partner within the school and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.

Top tips:

The options above are all genuine. Think through what is best for your school – the case study below may be helpful. As yet, there does not appear to be a common approach, but it appears a 'many schools to one DPO' model is emerging as the most common, whether that is provided by the local authority, or multi-academy trust.

Case study: Ark’s Data Protection Officer Solution

Ark has appointed an Information Governance Manager to serve as a MAT-wide data protection officer. This role supports Ark’s 36 schools, ventures, and central teams with developing data protection policies and processes and updating IT and data systems to enable their technical GDPR compliance. Training and support to designated data protection leads within each school will ensure that they can lead their schools in protecting staff, student and parent data.

To support cultural compliance, all staff will learn about GDPR and data protection as part of their annual induction, in the same way that they learn about safeguarding in schools and diversity in the workplace. Annual safeguarding audits will also be carried out at each school, to ensure that day-to-day processes across our schools meet the new data protection requirements.

Students will be required to give consent on the use of their data during secondary school, where consent is the condition in Annex 4.1 being relied upon, which will help ensure that they are educated in their rights as data subjects, as well as how to protect their own data, as part of the e-safety and digital/ICT elements of the curriculum.

By centralising the role of DPO across our network, Ark are reducing the burden on individual schools and supporting them in sharing resources and learning from one another on how to comply with the new regulations.

Relevant resources

- The European Commission sets out some guidelines on Data Protection Officers.

Step 8: Communicate with data subjects

Intended outcomes:

1. Be familiar with the full potential rights a data subject has, and the circumstances in which these do not all apply in all cases, in that exemptions exist.
2. Consider how best to **demonstrate** your compliance with new legislation, which is a key focus of what is changing. Compliance alone is not enough.
3. Be aware of 'exemplar' privacy notices for communicating with parents/pupils, and outline the work DfE is doing to test these with parents and the ICO on behalf of schools.
4. Gain benefits from being open and transparent with data subjects, there is more to building trust than compliance alone.
5. Subject access requests: key changes and tips for handling within schools.

How to approach this step:

- Be clear on who are the schools data subjects. Of course pupils are data subjects, but so too are staff, parents/carers and ex-pupils.
- The first thing to be aware of is 'what are key subject's rights?'
    - the right to be informed
    - the right of access
    - the right to rectification
    - the right to erasure
    - the right to restrict processing
    - the right to data portability
    - the right to object
    - rights in relation to automated decision making and profiling.

The right to be informed is a key part of the strengthened legislation. There are a number of ways that data subjects can be informed. These include:

- When providing 'initial registration' information upon joining the school. This is a big opportunity to get the data relationship right from the first contact.
- When providing additional information/data at various points during the year.
- Through effective use of the school website.
- In the case of staff, at various points in the 'lifecycle' of an employee, such as applying for a role, accepting a role/signing a contract, annual appraisals, upon conclusion of a contract etc.

But what does ‘being informed’ actually mean? It means the data subject receives clear communications about:

- what information is being collected/processed about them (in detail)
- why the data is collected (purpose)
- what the lawful basis for collecting and holding the data is (where applicable)
- who/which organisations data is shared with and why
- how the data is stored and how long for, and how security is ensured
- how to exercise their right of access to data
- how to exercise any other rights, such as restricting certain types of processing (for example biometric data) or to rectify data
- who to contact for queries

A Privacy Notice is one way of doing this, and some links to templates are provided in the resource section below.

The revised legislation requires that when the data subjects are children it should be written in a concise, clear and plain style. It should be age-appropriate and presented in a way that appeals to a young audience.

Data subjects have a **right to access** data. One way they can do this is through a **Subject Access Request**, which can be a request to see part or all of the data a school holds about their child.

Once they have seen that data, they may request it to be **rectified** if it is incorrect, and this is one area where subject’s accessing their data can help organisations. Regular (secure) checking of one’s own data can help with data cleaning and quality, which has other benefits to the school.

Finally, you should think about where some of these **rights are not going to apply due to other conditions set out in Annex 4.1**. For example, the right to erasure. Whilst the child is in your school, there may be data that you would not erase if requested. For example, if the parent asked you to delete all your children’s informal assessment data, then it would hamper your ability to perform your public task.

Top tips:

- Subject Access Requests (SAR) are not new within the 2018 legislation. The timeframe for response has shortened slightly (to one month, with exceptions). Schools do worry, “what happens if we get a SAR just before the summer holiday?” Education is largely unique in this regard, and the data protection legislation applies to all organisations processing personal data in the country. To efficiently deal with SARS the following tips may help:

    - Include your willingness to help data subjects access their data in your privacy notice. Explain to parents that most of the year you aim to do this in a timely manner, but during school holidays this may become more difficult.

- If you receive a SAR:
    - Have a conversation to see if the requestor is willing to clarify the scope of the data requested. A parent may only be interested in one small part of the data record, and would far rather get a quick response focussed on that scope rather than await a full SAR response.
    - Consider whether a SAR is complex. Whilst you still need to notify the data subject within 1 month if that is what you decide, it does allow you a further 2 months to produce the information. You must be willing to justify that decision and tell the requestor about that decision as soon as possible.
    - Check if this is an Educational Record request, as set out in The Education (Pupil Information) (England) Regulations 2005, as the timescales for doing so may be shorter.

- The revised legislation extends the need to inform data subjects about processing to children, not just their parents. Done well, this is a good thing, but it is wise to be cautious here. A communication that children don't fully understand could do more harm than good. (A child worrying why the school is collecting their test data and sending it off to the government for example). In particular with younger children, it may be that introducing such conversations within wider e-safety and ICT lessons is more appropriate. This then allows teachers to use language that suits their particular children, and ensure understanding and a 'chance to ask questions' is provided alongside the learning.

Relevant resources:

- Further information about the rights of individuals is provided on the ICO website
- DfE provides a range of model privacy notices for schools to adopt as one part of a schools communication with data subjects. These are currently being tested with groups of parents, and may well iterate in future as parental testing is combined with ensuring any edits remain aligned with legislation by checking in with the ICO.
- The ICO have also set out the minimum standards of privacy notices
- This simple 5 minute video prepared by GDPRiS provides parent focussed information that may be helpful in raising awareness amongst data subjects. There is an A4 printed sheet and infographic on the free resources section of their website.
- The European Commission have a pdf document online that sets out a lot of principles and good practice/bad practice examples in relation to transparency.

Step 9: Operationalise Data Protection, and keep it living

Outcomes from this step:

1. Identify the range of policies required within a school that cover the procedures and processes for data protection.
2. Understand what a data breach is, and what to do about it.
3. Ensure that data protection and risk management is a core and regular part of decision making and risk management practices within the school.

How to approach this step:

- The data that is processed, and the mechanisms through which your school undertake that processing, will evolve over time. The key things which need to be living documents to ensure they keep up with change are your:
  - data map/ecosystem drawing
  - data asset register
  - data protection impact assessment and risk management activity plan

- The Data Protection Officer will have views on how best to do this. It's about ensuring that the data protection principles outlined in your school's policies are embedded into processes within the organisation. For example:
  - Confirming that a new system has been recorded on the data map and data asset register should be an essential step before any procurement activity is concluded.
  - Each time data is shared outside the school, a 'check and send' culture to ensure that the data you are sharing, and who you are sharing it with, is logged centrally is good practice. Check that where appropriate a data sharing agreement exists and a record of the sharing is logged.
  - Ensuring the risk management work being undertaken feeds into overall risk registers and conversations with governors.
  - Ensuring that staff training is regular and appropriate.
  - Ensuring that you make the best use of 'key times' to communicate with data subjects, such as when first registering contact information.

- Operationalising the safe use of data on an ongoing basis requires a strong combination of safe people, safe technology, and safe processes. As such, ensuring that your school complies with the legislation requires looking across a wide number of policies that are used in schools today. Our working group has established the following (non-exhaustive list) of policies, which together help play a part in ensuring good management practices when it comes to data:

- Fair Processing or Privacy Notice – Pupils
- Fair Processing or Privacy Notice – Employees
- Data Protection Policy
- Data Retention Policy/Schedule
- IT and Communications Systems Policy incorporating:
    - roles and responsibilities
    - e-Safety policy
    - IT security policy
    - responsible user agreements
    - social media policy
    - trust website requirements and monitoring
- Code of Conduct
- Child Protection Policy (we have asked the local safeguarding board to review this)
- Business Continuity Policy
- Acceptable Use Policy: Employees
- Acceptable Use Policy: Pupils
- Acceptable Use Policy: Governors
- Data Breach Policy

Top tips:

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Some organisations may refer to this as a breach of confidentiality, integrity or availability, as this is how it is often referred to in many international information and security standards. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach may be about more than just losing personal data. The initial steps should be to minimise and assess the impact, and a range of different steps then need to be taken depending upon the severity, as set out in the ICO guidance.
- It is good practice to record and investigate every data breach, however small. An analogy here might be the ‘accident log book’. Whilst a child grazing a knee may be minor in isolation, if each incident is reported and a trend around a piece of playground equipment is spotted, some remedial action might be appropriate. And so it is with data protection: if a particular system or process is identified as regularly having minor incidents by the Data Protection Officer, they and the school can mitigate the risk. They can only do this if a ‘report it always’ culture exists and is encouraged.

- In the event of a serious data breach involving the personal data for which the controller is responsible the Data Protection Officer must report the breach to the Information Commissioner. A serious breach is a breach that interferes with the rights and freedoms of the data subject. This must be done within 72 hours of the breach.

Relevant resources:

- The ICO has guidance and templates to support schools undertake Data Protection Impact Assessments. (NB: under consultation at the time of creating this version of the toolkit).
- The ICO has a section on data breaches and sets out what to do when. If you are unsure how best to handle a breach they offer a helpline service to support you assess the impact and appropriate steps.

Annex

Annex 1: Explaining the language around data protection

Term	Description	Example
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data item	A single piece of information about a data subject.	"Ethnicity = white British" "Attendance = 97%"
Data item group	A group of data items that are typically captured about the same activity or business process in school. These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers.	Behaviour management, or catering.
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay, MyMaths.
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.
Personal data	Information relating to a natural identifiable person, whether directly or indirectly	John Smith was born on 01/01/1990. The head teacher's salary is £60,000.

Term	Description	Example
Special category data	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information. In education, it would also be best practice to treat things like FSM, SEN, and CIN/CLA status as special category data.	Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection.
(Data) Controller	The organisation who (either alone or in common with other people) determine the purpose for which, and the manner in which data are processed.	A school is often the data controller, sometimes a joint controller with the LA or DfE.
(Data) Processor	A person or organisation who process data on behalf of and on the orders of a controller.	A catering supplier the school uses.
Data audit/data asset register	The assessment of data and its quality, for a specific purpose. Other terms you might hear are data map or information asset log. In this context, we simply want the list of personal data assets that we hold, from which we can go on to place further important information alongside.	
Lawful basis and conditions for processing	These are the specific reasons, set out in law, for which you can process personal data. There is one list for personal data (lawful basis article 6) and another list for processing special category data (article 9).	"The processing is necessary for administering justice, or for exercising statutory or governmental functions." Read the full list.

Term	Description	Example
Data retention	How long you will hold information for to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of.	"We keep parent's phone numbers until 1 month after they leave the school in case of any issues that need resolving (for example, payment or repayment of lunch money) and then it is deleted."
Privacy notice	This is a document that explains to the people you have data about ("data subjects") the data items you hold, what they are used for, who it is passed onto and why, and what rights they have.	DfE publish model privacy notices.
Subject Access Request (SAR)	This is where a person (data subject), requests access to the information you hold about them. Timescales for responding, as well as reasons why you must comply or may refuse, as set out in law. A Subject Access Request is often used to describe "tell me all my data you hold".	"I want to know the attendance data you hold about my son"
Data Protection Impact Assessment (DPIA)	This is a process to consider the implications of some change you are introducing on the privacy of individuals. Assessing privacy at the outset helps you plan consultation/awareness/consent type options from the outset. "Privacy by design" is a term that is used in this space.	You would undertake one of these if introducing a new system to use fingerprinting within catering provision.

Term	Description	Example
Data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.	Sending a list of pupil names, attainment marks and dates of births to the wrong school.
Automated decision making/profiling	This is when machines/software apply rules to data and determine something about someone based on purely applying those rules. Typically it is the significance of the decision which drives the caution and concern here. Read further information.	“Anyone recorded as attendance >99% will get a voucher for X”

Annex 2.1: Table for identifying personal information to support the initial data map

	Do we receive personal data?	Do we create personal data?	Do we send personal data?	Do we destroy personal data?
Admissions				
Core management information system				
Curriculum tools				
Payment systems				
Virtual learning environments				
Catering management				
Safeguarding				
Trips and transport				
Uniform, equipment and photographs				
Identity management systems				
Contact/communication systems				
Social care and health interactions				
Statutory returns				
References and education settings you pass children onto				
Workforce systems				
Paper records				
Other				

Annex 4.1: The possible lawful basis and conditions of processing for personal data

The lawful basis for processing personal data

These are set out in Article 6 of the General Data Protection Regulation (GDPR). At least one of these must apply whenever you process personal data:

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

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

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

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

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

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

Where you are processing **special category data,** set out in Article 9 of GDPR, **as well as** one of the six lawful basis for processing, you must ensure that a **condition for processing** from the following list applies:

a) **the data subject has given explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

b) processing is necessary for the purposes of **carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

c) **processing is necessary to protect the vital interests of the data subject or of another natural person** where the data subject is physically or legally incapable of giving consent.

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

e) processing relates to personal data which are manifestly made public by the data subject.

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) **processing is necessary for reasons of substantial public interest,** on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) processing is necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i) processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Schools will also need to know and rely upon the additional conditions for processing special category in Schedule One of the Data Protection Bill, when finalised.

Annex 5.1 An Emerging Data Retention Strategy for the sector

It is clear from work done so far that the sector is some way off having one 'standard' data retention set of standards. Whilst 'one policy' for the sector may never quite be achieved, most would recognise that there is benefit in greater harmony than we have at present within our sector.

This is an area of this document that is very much a 'work in progress'. **We would welcome feedback and how we can work up the thinking set out below into something that grows into an authoritative set of recommendations. For now, we recommend what is below to stimulate thinking and consideration of your local practice, but we do not recommend that any firm decisions are taken on the back of this guidance alone. It remains for each school as a data controller to set the data retention schedules that work for them and are justifiable.**

We have introduced that data items aggregate into data item groups. Whilst thinking at data item group level allows us to have a sensible conversation, it should be noted that the data item group 'Personal identifiers, contacts and pupil characteristics' generally sits within all other data item groups:

Personal identifiers, contacts and pupil characteristics
Admissions
Attainment
Attendance
Behaviour
Exclusions
Identify management and authentication
Catering and free school meal management
Trips and activities
Medical information and administration
Safeguarding
Special educational needs

The following table sets out the emerging thinking from a sector working group discussing data retention in schools. This is provided as an illustration of the types of justification schools might want to consider. Further work is needed to test and iterate these justifications. Schools should continue to develop and own their own data retention policy based upon local justification and necessary task.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Admissions		X (admissions files)	X (admissions appeals)		**Admissions files** Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. It is then used for some validation and cross checking of enrolment details. Once enrolled, the child's records in the MIS become the core record. Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it (for example, where in the city children are interested in our school, or the SEN make up) is aggregated within the first year to a level being non-personal, after that, the detailed data within the admission file could be deleted. It is important to retain detailed data for a year, any appeals for which richer data about other

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					successful/unsuccessful appeals may be relevant typically happen in the first year. **Information about admissions appeals** When dealing with appeals, having a reasonable history of any other appeals in some detail can be needed to deal with the particular appeal. The information is needed alongside the admissions policies of the time.
Attainment			X		Formative assessment data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention. Summative attainment is the main outcome of what children 'attain' in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is 'passed on' smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					data for 1 year after the pupil has left the school feels proportionate. Trend analysis is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity. After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.
Attendance		X			Attendance data probably resides in some 'operational' systems in schools, such as cashless catering. In these systems, the data should only be retained until the associated business processes have concluded (for example, payment of meals). The start of the next academic year once all bills are settled feels proportionate.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child. After that period, non-identifiable summary statistics are all that is required to support longer-term trend analysis of attendance patterns. We noted another GDPR principle here that may apply to attendance. Under data minimisation, where ‘paper records’ capture attendance, this paper record duplicates the electronic version and is probably required once the paper has been transferred to a stable electronic format.
Behaviour		X			This is all relevant for managing children when with at your school. 1 year allows a period of ‘handover’ to next institution with conversations supported by rich data if relevant.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Exclusions		X			Exclusion data should be 'passed on' to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.
Identity management and authentication	X (images used for identity management)				
Catering and free school meal management		X (meal administration)	X (free school meal eligibility information)		A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically 'one month' may not be enough, but 'one year' feels enough. Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7-

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					year record also needs to be portable with the pupil, as historic dates can be used for funding.
Trips and activities	X (field file) X (educational visitors into school)		X (financial information related to trips)	X (major medical events)	Financial information related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions. A 'field file' is the information that is taken on a trip by a school. This can be destroyed following the trip, once any medicines administers on the trip have been entered onto the core system. If there is a minor medical incident (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school') on the trip, then adding it into the core system would be done. If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate. Permission to go on the trip slips will contain personal data, and destroying them after the trip

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					unless any significant incident arises is appropriate, otherwise refer to the policies above. Schools sometimes share personal data with people providing ‘educational visits’ into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.
Medical information and administration	X (permission slips)	X (medical conditions and ongoing management)		X medical incidents (potentially)	To support any handover work about effective management of medical conditions to a subsequent institution. Permission forms that parents sign should to be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time, that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent. Medical ‘incidents’ that have a behavioural or safeguarding angle (including the school’s duty of care) should refer to the retention periods associated with those policies.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Safeguarding				X	All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records.
Special educational needs					
Personal identifiers, contacts and personal characteristics	X (images used in identity systems) X (biometrics)	X (images used in displays in school)	X (postcodes) X (names) X (characteristics)		Images are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent captured at the outset of using the photograph. Biometric data (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
	X (house number and road)				after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal). As set out in other sections, names are needed for smooth handover to subsequent schools for up to one year. Postcode data is useful in analysing longer-term performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity. Schools may well provide references for pupils for up to 3 years after they leave, and so retaining the name in the core pupil record is important (this doesn't mean it needs to be retained in all systems). Keeping names attached to safeguarding files for longer than this may be entirely appropriate – see safeguarding section. Characteristics form an essential part of trend analysis, and so retention is in line with those needs.

When setting data retention policy, it is good practice to not only create the written ‘plain English’ justification, but also set it alongside the legal basis for processing, set out in step 4.

Data retention should also be communicated ‘as a whole’, so the data subject is as informed as possible. So, importantly, a school data retention document may describe exactly when a school destroys personal level data, but the school should take steps through privacy notices to ensure that the data subject is aware of where else the data has been sent, and ideally signpost to the data retention policies associated with that sharing.

DfE is aware that several schools make reference to the IRMS Toolkit when setting data retention periods. The IRMS is a not for profit organisation that supports the Information and Records Management Profession. As part of their current model they make some content available open source. The data retention element of that toolkit has many strengths, in particular the links with related legislation and the fact that it has evolved over time with significant input from people involved in the administration of education who are members of the IRMS.

Depending upon the feedback during the initial consultation period, it is probable that further work will be done to develop a consistent voice that supports schools by generating and sharing exemplar data retention policy.

Annex 6.1 Example Data Protection Impact Assessment template

Data set/system	Current practice	Impact of threat if occurs: 1=low 5=high	Likelihood: Low, medium, high	Response to risk	Action plan	Review date
Name the data set and/or system with personal level data	What current practices exist (or not) that could either lead to the threat materialising or prevent the threat from materialising? For example, data entry, data management, transfer of data, collection of data, printing and storing information, handling data	Identify what **potential threat** could be realised. Is threat related to: • Privacy breach (data shared w/o consent or disclosed) • Individual – in danger of harm/potential embarrassment /loss of confidentiality/ discrimination • System failure or technical issues • Non-compliance with GDPR through inadequate procedures/ non-consent/ negligence/	As a result of practice, how likely is the identified threat a reality? Select from: Low Medium High	Transfer risk to third party/insurance Treat/mitigate Risk - reduce risk Tolerate/accept level of risk Terminate/remove risk	Where the likelihood of a threat is high or medium, identify the actions to address the threat and mitigate or minimise the risk if not eliminated What actions can be taken to minimise the risk or eliminate the risk altogether? In some cases, threats cannot be removed entirely in which case, can agree action to 'Accept risk – no further action necessary' Ensure actions have lead person identified, timelines and linked	Depending on Action taken plan for a review

Data set/system	Current practice	Impact of threat if occurs: 1=low 5=high	Likelihood: Low, medium, high	Response to risk	Action plan	Review date
		disregard/ ignorance/data shared without consent/data loss			actions that impact upon the overall action to mitigate or eliminate the risk.	

Annex 10. Lead Contributors

This toolkit has been put together as a result of significant contributions and collaboration between a number of individuals representing many perspectives. The Department for Education is particularly grateful to people from the following organisations for giving their support:

Organisation
Information Commissioner's Office
Oxford Diocesan Schools Trust
Ocean Learning Trust
Independent School's Bursars Association
Ninestiles Academy Trust
Ark Academy Trust
Hockliffe Lower School
Broadmead Lower School
Bedford Catholic Schools (SFAAT)
South West Grid for Learning
Dobcroft Infant School
Edith Cavell Primary School
Beaudesert Lower School
The Independent Schools Council
Queen Elizabeth High School, Lincs
Boston High School
Flitwick Lower School
Edith Cavell Primary School
Thomas Johnson Lower School
Defend Digital Me

Organisation
Lincolnshire County Council
Capita SIMS
GDPR in Schools (GDPRiS)
CBICT Ltd
Assembly
TheTrustBridge
Michelmores
National Centre for Cyber Security
Information and Records Management Society

Department
for Education

About this publication:
enquiries www.education.gov.uk/contactus
download www.gov.uk/government/publications

Reference: DFE-00119-2018

Follow us on Twitter:
@educationgovuk

Like us on Facebook:
facebook.com/educationgovuk