FORM

GDPR audit

Work through our audit to help you make sure your current data processing arrangements:

- Comply with data protection law
- Are in line with best practice

Mandatory documents or tasks are highlighted in blue, the rest is good practice. Remember that:

- This list isn't exhaustive to every type of non-statutory document or arrangement you might have or need, so add in new sections for anything you think is needed in your school (your analysis of data processing risks should help you figure out what else to put in place – we explain how to do this in the 'Data processing' section below)
- If there are non-statutory parts of this audit that you know you can't reasonably accomplish in your school, that's fine. You can either remove them or make a note in the 'future actions to be taken' about why they're not currently achievable

You can RAG rate each of the processing and security arrangements to demonstrate how far along you are with meeting each measure. For example: red = 'not done', amber = 'in progress' and green = 'complete'.

We wrote this audit with the help of Sharon Graham, our associate education expert.

Sharon Graham is DPO for 3 schools, and runs a GDPR working party for DPOs. She also has 10 years' experience in the education sector covering all aspects of operational management.

Documents

For each document below:

- Check the links for a template or guidance if you need help creating it
- If you already have it, make sure your version meets the requirements or best practice by comparing it with our template or guidance
- Ask yourself:
    - Is it up-to-date?
    - Do members of staff know where it is if they need to use it?
    - Have you had any issues or complaints about using or understanding the documents (e.g. parents have complained about privacy notices not being clear)
- Note down any changes that are needed in the table

DOCUMENT NAME	CHANGES NEEDED	PRESENT (✓)
Record of processing activities	*Check whether you're satisfied that the 'lawful bases' and any conditions of processing you use are the appropriate ones, and that any safeguards you've used to transfer data internationally are suitable*	
Privacy notices	*Consider whether you have notices for all members of your school community (e.g. staff, governors, volunteers, pupils, parents, etc.)*	
Contracts with suppliers if they're data processors	*Data processors are any organisation that processes data on your behalf (e.g. payroll providers). Make sure your contracts with all of your data processors meet the requirements*	
Record of data breaches	*Pay particular attention to the outcome of breaches, making sure they were handled appropriately*	
Consent forms (where needed)	*Consent is only needed when no other 'lawful basis' could apply. These forms should allow you to obtain consent to the standard required by the GDPR*	
Data protection impact assessments (where needed)	*These assessments are only needed when introducing new technologies to your school with a high risk to data protection rights (e.g. a new CCTV system)*	
Information audit	*Doing this will make it easier to complete your record of processing activities - although there's no need to keep this up-to-date if your record of processing activities has been updated*	
Data protection policy		
Retention schedule	*This'll help you complete the 'Records management' section below and make sure that you 'don't keep data for longer*	

DOCUMENT NAME	CHANGES NEEDED	PRESENT (✓)
	than necessary'	
Data breach procedure	*Typically this process will involve making the DPO aware of any breaches. Check your data protection policy to see if this is set out*	
Record of any 'legitimate interests' assessments you've conducted		
Record of consent		
IT and acceptable use policy for staff		
Record of subject access requests received and completed	*Pay particular attention to the outcome of requests, making sure they were handled appropriately*	
Record of what personal data has been destroyed		
Record of what copies of personal data have been taken off site (for documents containing detailed data, unlike exercise books)		
Register of school IT hardware (including office equipment and mobile devices)		

Data processing

Check these with your data protection officer (DPO), or anyone else who leads on data protection on a day-to-day basis.

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
We have an appointed DPO			
If our DPO is external to the school, we also have a data protection lead who can help oversee data			

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
protection compliance on a day-by-day basis			
We have issued privacy notices to anyone whose data we process	*If you're not certain, talk to whoever is responsible for collecting data and ask them to show you how they make sure people are made aware of privacy notices on any data collection sheets or systems used*		
We have issued consent forms when we need to rely on this as a lawful basis to process data	*Check your record of consent, and make sure your consent forms are appropriate (see the 'Documents' section above)*		
Our DPO makes regular reports to governors			
We have assessed the risk presented by our processing to help us assess the appropriate level of security to put in place	*The assessment should consider:* • *The nature and extent of your school's premises and computer systems* • *The number of staff you have and the extent of their access to personal data* • *Any personal data held or used by a data processor acting on your behalf* *Read more about this in ICO guidance*		
We have processes in place to allow individuals to: • Make a subject access request • Exercise their other rights over the processing of their personal data (e.g. right to erasure or right to correct data)	*Typically this process will involve forwarding these requests to the DPO or data protection lead at your school. Check your data protection policy to see if this is set out*		

Records management

Speak to your administrative staff about these tasks, as they're usually responsible for them. Your record of disposal should also be useful.

Personal data should be kept for no longer than necessary. Your retention schedule will define what a 'necessary' time period is.

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
An annual check on the personal data we hold has been done			
Records have been disposed of in line with our retention schedule			
Records have been disposed of securely (e.g. using a cross-cut shredder, not leaving records in a regular waste bin)			
Records have been looked through to make sure we're not keeping unnecessary data			

Security of physical documents

Conduct a spot check to test out whether these elements of good practice are followed.

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
Copies are put away if someone is not in the room (a 'clear desk' policy)			
Copies are kept in locked cupboards or cabinets, with keys kept in a secure location in the school			
Access to copies is limited by role (e.g. finance managers likely won't need to see safeguarding	*Ask your staff who has access to the keys to locked cupboards*		

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
information)			
All adults on site wear IDs, and visitors are signed in and out			
All doors to offices are kept locked when not in use			
All windows are locked when rooms are not in use, with a restrictor installed			
Displays containing personal data only show the essential information	*For example, consider whether you need full names and photos of pupils on display*		
Displays containing particularly sensitive data, like medical information are kept away from public areas (e.g. keeping them in the staff room or kitchen)			
The above sensitive displays are covered up or removed when locations are used by external groups			
Screens aren't visible through windows			

Security of electronic documents

Do a spot check and ask staff if they're currently embedding these practices, and talk to your IT staff about your current IT arrangements (e.g. about whether your equipment and email system is encrypted).

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
Computers are locked when not in use, with an automatic lock time of 15 to 30 minutes for administrative staff			

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
Access to documents on the school system is limited by role (e.g. finance managers likely won't need to see safeguarding information)	*Ask your IT staff to show you who has access to what files and check those access lists are appropriate*		
Password protection is in place for computers			
Particularly sensitive documents are password protected			
USB ports are locked down to prevent data being taken out of the school without permission	*A remote access system is preferable (see the 'Working remotely' section below)*		
Any computer hard drives, USB drives or laptops that are used are encrypted			
Email addresses are always double checked when sharing data, with autocomplete functions for entering addresses turned off			
Emails containing particularly sensitive data are encrypted			
Emails are checked before opening attachments or links to avoid viruses or phishing			
Emails containing personal data aren't sent to staff members' or governors' personal email addresses			
Printers and copiers are password			

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
protected			

Working remotely

Ask staff who work from home or run school trips if they're currently embedding these practices.

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
Physical copies are stored in a secure area or case, and aren't left on transport			
Personal data isn't saved on staff members' personal devices, but instead viewed through a remote access portal (check log-in details to make sure)	*If you don't have a remote access system in place, it's recommended rather than using less secure systems like USB drives to take personal data off-site*		
Any devices used for remote access are password protected, locked when not in use, and windows are closed when no longer needed	*This will be difficult to produce evidence for, but you may want to ask staff to bring in their personal devices and demonstrate how they use them to access data remotely*		

Training

For this section, assemble a sample of staff members, governors and volunteers with a mix of seniority and experience, so you get a full picture of how much the school community understands with regards to data protection. If you have someone responsible for data protection training you should also ask them.

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
We have someone responsible for data protection training for staff, governors and volunteers			
We deliver training annually, or more often if gaps in knowledge			

TASK	EVIDENCE OF STEPS TAKEN SO FAR	FUTURE ACTIONS TO BE TAKEN	RAG
are identified			
We follow-up on training to ensure understanding, such as through a short assessment exercise			
Staff and governors have read our policies related to data protection (see 'Documents' section) and know which one to look at if they have a question	*Is there a process for new starters to read these policies?*		
Staff and governors are confident that they know: • What a data breach is and how to report one • How to recognise a subject access request and what to do if they receive one • What to do if they want to share a piece of personal data externally, including if it's shared internationally • How they should access and use personal data if they want to look at it away from the school site			