The implementation of GDPR in the education sector

Analysis of operational risks in the schools and academy trust sector

January 2018

wardhadaway lawfirm

Newcastle | Leeds | Manchester

SCHOOLS NORTHEAST

The future of our region is in school

COMMERCIAL SUPPORTER

Background to this risk analysis

Ward Hadaway has a significant education practice with clients across virtually all stakeholder groups in the sector. On 11th and 13th July 2017 we presented "Preparation for GDPR Workshops for the Schools and Academies sector". These events focussed on the steps to be taken toward ensuring an organisation can be compliant with data protection laws at the date of GDPR implementation (25th May 2018). A similar event was held in April for Local Authorities in the West Yorkshire area and whilst that event covered a wider agenda, considerable time was afforded to the specifics of implementation of GDPR in the area of Childrens' Services.

During the autumn term further sessions were undertaken with more than 200 school leaders, business managers and, importantly also, Governors and Academy Trustees. Within the discussions and questions that ensued, we captured some common themes in terms of risk issues that the Schools and Academies sector perceive are likely to exist. These can become significant challenges as the education sector moves towards the deadline for implementation.

We also felt it important to understand the Department for Education's approach to implementation in the School sector. We've been able to meet with the Head of Data Strategy for DfE and have had a brief discussion with a participant in the department's internal working group, tasked with the development of the department's policy position on GDPR compliance in the School sector – a group that is expected to issue guidance in the foreseeable future.

We see the education system as highly respectful of rights of individuals which are upheld through the regulatory regime. By its nature regulation imposes burdens in terms of time and cost for organisations that are already subject to many competing claims on time and finances. This to a background of the importance of prioritising as much resourcing as possible to the area of education services and the delivery of high quality and impactful education.
We can also see areas of working practice where third party applications subscribed to are not necessarily in line, currently, with good practice incorporating in particular the principle of privacy by design. The entire education sector data protection landscape is far from complete in the context of new and more sophisticated compliance duties that will come into force on 25th May 2018.

To this background Ward Hadaway has prepared this operational risk analysis for reference within the sector. We've looked in some depth at the way Schools, Academies and their Trusts operate and within these operations hold, use and provide to others personal data in an identifiable format. This document will be updated in the light of the continuing dialogue that we have with Schools, Academies, Local Authorities and suppliers (particularly those working within the EduTech space) in the coming weeks. We are particularly keen to reflect DfE guidance as that is issued. Any guidance (including that produced by the Information Commissioner's Office) will be taken into account in future versions of this document.

Please be aware that this document cannot be comprehensive of all circumstances and scenarios that might arise. The paper must not be relied upon as representing legal advice.

Operational risk analysis

Ref no	Subject	Risk issue to be considered	Reserved for notes	Actions required
1	**Governance and GDPR compliance**	The Board of Directors of the Trust/Governing Body of the School/School Federation must be sufficiently aware of the responsibilities GDPR brings and the financial and reputational risks attached in order to respond appropriately and effectively when circumstances require. The Board is also expected to fully support the appointed Data Protection Officer in the performance of that person's role.	Appreciation of the role, duties and particular employment status of the Data Protection Officer is essential. Ensure there is appreciation of the increasing significance relating to the management of data protection issues and that an effective communication line exists for the Data Protection Officer both to the Board/Governing Body and to all parts of the organisation. The Board/Governing Body may, for smaller organisations, consider authorising an outsourcing of the role but will need to understand how this is to be achieved and whether an appropriate allocation of risk is capable of being achieved.	Brief the Governing Body or Board or Trustees on the Data Protection Regime. Develop a reporting mechanism to identify who the Data Protection Officer reports to at Board level and develop a template for, we suggest, quarterly reporting to the Board/Governing Body.
2	**Compliance in LA maintained schools**	The School governing body is the relevant body for compliance purposes. Governing Bodies already carry various regulatory burdens – notably child protection and health and safety – but the compliance obligations under GDPR are particularly prescriptive requiring the Governing Body to ensure that it has appointed a Data Protection Officer.	Sharing of a DPO is permitted across several parties subject to the obligation. Following an already existing European model the role can be outsourced. DfE will wish to consider the risk over the coming months of opportunistic businesses soliciting contracts from Schools but where the service provider lacks all necessary competencies. .	Fundamental is the duty to appoint a DPO. If outsourcing is not regarded as appropriate for any reason (e.g. through inability to secure an appropriate allocation of risk on an affordable basis) there may need to be compromise over the avoidance of conflict of interest duty. Consider what mitigation strategies can be developed and ensure that the Board is fully briefed on the position and

			There should be consideration of a quality assurance process to ensure that competency in handling compliance issues in the education sector can be taken as a given. For smaller schools it may be impossible to identify a DPO that is complete clear of conflict of interest issues.	takes a monitoring role over this issue going forward.
3	**Scope of compliance responsibility**	A MAT operating a trading company and any School managing leisure services for a local authority will need to consider the compliance responsibilities associated with those operations.	A trading company will have its own responsibilities independent of the MAT. Its Board of Directors must ensure that it has systems in place assuring the organisation of compliance. Where local authority leisure services are managed by a School or MAT care should be taken to understand respective data protection obligations and develop an appropriate compliance regime.	Ensure that any trading company board of directors is appropriately resourced to manage its data protection responsibilities. For leisure services agree appropriate arrangements which are likely to require a formal data sharing agreement.
4	**Capacity - resourcing**	Resourcing to implement any organisational change that may be necessary. Several activities below imply that significant resourcing (finance and human) are likely to be required to be committed to GDPR implementation and thereafter ongoing compliance.	Academy Trusts will have signed off budgets for 2017/18 and most are unlikely to have made provision for (potentially) an additional staff member to act as Data Protection Officer, staff training and legal advice to support policy changes/new policies to meet compliance obligations.	Designate a Data Protection Officer and determine the scope of the role. MATs will also need to address what communication lines will exist between schools and the MAT leadership team/Data Protection Officer to encourage and as necessary enforce strong compliance at all levels within the organisation. Take into account the resource implications of data protection compliance in the preparation of the 2018/19 budget.

5	**Privacy notices**	DfE has revised its template privacy notice. This requires carefully considered local development to ensure that it provides information that is specific to the organisation that operates the policy.	There are further privacy notices/policies required that extend beyond the scope of the DfE template eg in relation to personal data obtained as part of a recruitment exercise.	Ensure that in the period to May 2018 there is clarity around the extent to which notices are required and ensure these are developed. Legal advisors providing compliance toolkits will be able to support this exercise.
6	**Systems vulnerability**	Data protection laws already impose compliance requirements in the area of information security. GDPR reinforces this aspect and creates a more significant financial penalty regime. Many schools may have no encryption functionality. We also learned of schools that do not have immediate access to email encryption functionality meaning that when data is transferred to e.g. Childrens' Services the service of an encryptor is purchased at a per email charge. We understand that third parties such as GroupCall may for convenience encourage schools to provide administrator rights to access data in real time as a live user of the system with no school management or ability to monitor.	By way of example of issues to be addressed, current DfE advice on MIS Procurement recommends the option of assembling a system from various products sourced from different suppliers. MATs and Schools need to assess and address any weaknesses that make systems vulnerable to hacking and other criminal activity. It may become increasingly essential to have a single provider with overall responsibility for the security integrity of systems used. Schools should be strongly advised to restrict data extraction by reference to a detailed agreement on the precise data that may be accessed, the purposes for which data is used in processing and for how long it will be retained.	Contract terms with third party suppliers who receive and process identifiable personal data must be compliant with GDPR and specific requirements in the context of education services should be taken into account. Monitor supplier activity in this area. If there is no evidence of suppliers updating their standard terms and conditions prompt for this action to be taken. NB Auditing of supplier's procedures is likely to become part of good practice in the sector but there is a need for this to be undertaken on a basis that ideally avoids multiple requests being made of the same supplier – potentially with different requests for information. Ward Hadaway awaits understanding DfE's position on this before proposing audit material.
7	**Management of compliance generally**	Circumstances in which a breach of data protection laws arise will in many cases occur at local level eg in a MAT school. There is a risk that notifications do not happen at all or notification is late if there fails to exist a strong relationship between the MAT head office team and its schools.	Reporting of a breach should be undertaken within 72 hours. Weekends and Bank Holidays are included in the calculation but a reasonable application of this requirement is expected to be taken by the ICO.	Local "buy in" to data protection compliance will be essential. Ensure that breach notification procedures are developed to enable timely and appropriate responses to be carried out.

			It will be prudent for each individual school within a MAT to have a designated individual with responsibility for compliance and with a duty to make the necessary notification to the MAT head office function. A relatively sophisticated understanding of data protection laws will be vital if that responsibility is to be correctly discharged. Note that the ICO is due to issue consultation proposals for a revised Regulatory Action Policy. This will inform its decision making and the administering of sanctions. The education sector will be keen to provide input to the consultation exercise for obvious reasons.	
8	**Compliance in LA maintained schools**	The School governing body is the relevant body for compliance purposes. Governing Bodies already carry various regulatory burdens – notably child protection and health and safety – but the compliance obligations under GDPR are particularly prescriptive requiring the Governing Body to ensure that it has appointed a Data Protection Officer. We are awaiting the DfE position statement on this.	Sharing of a DPO is permitted across several parties subject to the obligation. Following an already existing European model the role can be outsourced. DfE will wish to consider the risk over the coming months of opportunistic businesses soliciting contracts from Schools but where the service provider lacks all necessary competencies. There should be consideration of a quality assurance process to ensure that competency in handling compliance issues in the education sector can be taken as a given. For smaller schools it may be impossible to identify a DPO that is completely clear of conflict of interest issues.	Fundamental is the duty to appoint a DPO. If outsourcing is not regarded as appropriate for any reason (eg through inability to secure an appropriate allocation of risk on an affordable basis) there may need to be compromise over the avoidance of conflict of interest duty. Consider what mitigation strategies can be developed and ensure that the Board is fully briefed on the position and takes a monitoring role over this issue going forward.

9	**Management of child consents**	There are requirements imposed upon schools and academy trusts to hold and in many cases make transfers of data to third parties – typically also in the public sector. The Prevent strategy presents particular challenges in compliance terms.	Schools and academies should seek to base data processing so far as practicable and legitimate under data protection laws on grounds other than consent. Where consent is necessarily the correct basis of operating, ensure that actions are taken based upon valid up to date information and that arrangements involving data sharing are explicitly covered within any consent obtained. Detailed documentation of the consent and retention of the consent record will be important considerations.	See also item 12 below.
10	**Impact of duties and relationships with the wider public sector**	There are requirements imposed upon schools and academy trusts to hold and in many cases make transfers of data to third parties – typically also in the public sector. The Prevent strategy presents particular challenges in compliance terms.	Ensure that there is clarity around data transfers that arise under legal obligations e.g. with DfE. Consider whether there should be an appropriately drafted data sharing agreement in place with other public bodies. The Prevent strategy includes duties not to disclose certain matters. The duty impacts upon the private sector e.g. ICT Suppliers and School Improvement service providers who provide supporting services for schools and academies.	Ensure that the organisation has appropriate arrangements in place for the transfer of data to other public bodies. This may be through legal duty or a data sharing agreement.
11	**Auditing of data held and developing an accurate record of purposes for which the data is held.**	This is a core requirement of data protection laws. Organisations with 250 or greater employees must maintain a formal record of the types of personal data held and for each data item the purposes for which it will be used.	This issue requires most immediate attention within Schools and Academies as completion of this exercise will aid an appreciation of what data is held and why, what data is processed and for what purposes and that there is a legitimate basis	Schools and Academy Trusts affected must set up a register of data held meeting the requirements of GDPR and have a system in place involving ownership and processes for updating.

			upon which the information has been collected and is retained and processed.	
12	**Relationships with service providers present schools with additional compliance requirements**	Increasingly data requires to be passed by the school to a service provider to enable student set up on apps that the student requires access to. The process of transfer requires compliant management. Education suppliers may not have access to information to validate that the data it is receiving is accurate and that the information has been passed to it in compliance with data protection laws.	There will be complexities around the status of consents given (by parents for younger children) with there being at all times the possibility that consent is withdrawn. Age verification will also be a significant issue. Note that a UK Government decision on the setting of the consent age (currently 16 but with the possibly of it reducing to any age not less than 13) is a relevant issue for the sector.	Contracts with suppliers involved in the processing of personal data controlled by the school or Academy Trust will need to be GDPR compliant. Schools and Academy Trusts should expect suppliers to address issues and challenge them if they do not. Where personal data is to be legitimately accessed by the Supplier ensure the agreement includes a pro-forma schedule of the data required. If the Supplier is provided with administrator rights to access data in real time identify whether it is technically feasible to limit the scope of that access right. In any event, ensure that the contract terms provide strong protections for the school against inappropriate access and the consequences that could arise – including an indemnity covering financial liabilities.
13	**Data that is to be legitimately transferred to another party cannot be transferred independently of a larger data set.**	The data transfers enabled through applications subscribed to may be excessive and include personal data that is linked to the information to be transferred but not required for the purposes of the data processing instructed.	Certain applications facilitating data exporting do not incorporate functionality that allows for the selection of particular data sets/individual data elements. This means that all data recorded on the system against a data subject must be exported as an aggregated data transfer.	Consult with any supplier who is unable to facilitate selective data exporting. It is likely that the supplier will be further developing its product to facilitate selective exporting. In future the duty to incorporate "Privacy by Design" will become a key factor in the development and selection of IT products and services involving personal data.

				Consider current and possible future projects to be undertaken. Identify if the project involves in any way personal data and ensure that a privacy impact assessment is considered and if appropriate implemented.
14	**The duty to undertake privacy impact assessments**	GDPR reinforces the significance of impact assessments where major developments occur that create the potential of additional risks of misuse of personal data. Judgements will be required to be made as to when to undertake an impact assessment.	A decision to form a new MAT with the involvement of say 10 Schools is an obvious example where an impact assessment should be undertaken. There will be less clear examples e.g. school rebrokering with a school transferred from one MAT to another. Guidance in this area is likely to be helpful to Trustees and Governors.	Consider current and possible future projects to be undertaken. Identify if the project involves in any way personal data and ensure that a privacy impact assessment is considered and if appropriate implemented.
15	**Profiling using student data**	Profiling is increasingly accepted as an effective tool to analyse student performance, establishing in the process appropriate interventions. Profiling and the management of the outcomes is a particularly sensitive area to be managed by MATs and schools.	Transparency in this activity will be vital. There is the prospect of the need to update policies and privacy statements and consider whether existing published statements as to the purposes for which data will be processed adequately allow for the implementation of new profiling initiatives. The DfE template notice requires, in our opinion, more detailed development in this area.	Ensure that your published privacy notice includes appropriate reference to profiling. Ensure that the outputs from profiling are treated as further personal data to be retained in accordance with data protection procedures.
16	**Relationships with suppliers –contract terms**	GDPR sets out a series of principles that require to be complied with by data processors. This should be translated into formal contractual undertakings by the relevant supplier.	New contracts should be compliant. Existing contracts should where relevant be varied to include updated GDPR compliant duties.	See point 9 above.
17	**Insuring of risk**	Many commercial organisations are able to effect insurance against certain risks such as cyber threats albeit with compliance requirements	Many Academy Trusts now commit to the Risk Protection Arrangement sponsored by the Department. DfE should be expected to set out its	Consider whether commercial insurance could be appropriate for your organisation in relation to data protection risks.

		in relation to the security standards implemented with the organisation.	position in this area as interest in insurability grows. DfE guidance awaited.	
18	**Archiving**	Data held by schools and academies is frequently retained without detailed consideration as to the basis for doing so. Retention periods for certain information will be based upon DfE requirements/expectations which in certain cases are supported by legislation. .	Ensure that data retention policies are in line with the requirements of DfE and any other legal obligations the school/academy may be subject to. Contractual terms and conditions of suppliers will typically also establish required retention periods. These should be aligned with the Schools policies relating to data retention where personal data is involved. .	Develop or update data retention guidelines that operate within the organisation ensuring that these are compliant with data protection duties. Ensure that under the transparency duty there is clarity around retention periods and apply these across the organisation. Where data is backed up consider your policy for the periods during which backups are retained.
19	**Right to be forgotten**	The right to be forgotten requires a good understanding of the legal basis under which the right can be enforced and the circumstances in which a duty to erase data will not arise. Schools and Academies will want to be clear that the right when exercised cannot compromise the necessity of holding, maintaining in up to date form and processing of personal data in the course of providing education.	Procedures should be put in place to refer any request to an appropriate individual involved in records management. The procedure should encourage reference to the Data Protection Officer for guidance given that requests of this kind should only arise on an occasional basis.	Ensure that the Data Protection Officer has a good appreciation of the legal requirements.

Further details

This paper has been prepared by Ward Hadaway to encourage wider interest in the issues we have identified. To discuss any aspect of data protection law compliance, please feel free to get in touch:

Frank Suttie
Partner | Commercial

E: frank.suttie@wardhadaway.com
T: 0113 205 6783
M: 0778 6 11 4 339

Graham Vials
Partner | Employment

E: graham.vials@wardhadaway.com
T: 0191 204 4383
M: 0752 580 2955