Countdown to GDPR webinar – 11th July 2017
Questions and answers

Question/Comment	Answer
Is GDPR going to replace the DPA completely?	Yes, absolutely. The DPA came in to force in 1998; the idea of GDPR is that it is a regulation that has direct effect across all EU member states. Each country within the EU will be subject to exactly the same wording from the regulation. It is seeking to remove the DPA, or country equivalents, state-wide nuances and different interpretations; GDPR will eradicate all of this and everyone will comply with the same regulation. This is subject, of course, to Brexit but the UK will continue for the next 2 years at least in compliance with this.
Where do we stand with data in Office 365 and G-Suite? I take it they will be GDPR compliant?	While the applications may be compliant themselves – refer to Microsoft or Google's GDPR compliance statements for this – schools are the data controllers of what is stored in O365 and G-Suite. What you store is your decision and if it contains personally identifiable data, it must comply with the 6 pillars of personally identifiable data.
As regulation does that mean any company (including educational institutions) is subject to an audit at any stage?	The ICO has the power to investigate data breaches and fine organisations for non-compliance with the DPA. That will continue with the GDPR.
Does GDPR have less conflicts than are potentially possible with FOI?	GDPR and FOI are different things. GDPR affects schools and educational establishments in how you process personal data – much the same way as it was under the DPA, so you should already be compliant – it's all about the data you collect, what you use it for, how it is retained, how you delete it, and ensuring you have consent for that process. The FOI act different because it is about schools giving information about, for example, the contracts that you entered into. Anything commercially sensitive in those contracts would be redacted. They are both relevant pieces of legislation but different so your obligation of reporting under the FOI will not be impacted by GDPR.
Will this finally be the end of non-encrypted memory sticks?	We certainly hope so. Update: why use USB memory sticks at all? While you may be able to force encryption using BitLocker (https://technet.microsoft.com/en-us/library/jj679890.aspx), a

	better alternative to unmanaged storage devices would be to use a secure cloud storage solution such as Microsoft OneDrive or Google Drive.
As the controller of the information and with GDPR how does this affect how we share the information with 3rd parties? I.e. Police.	Ensure all personal data you share is encrypted. If the Police gives you a RIPA form you must complete it; it is always good practice to give due consideration to it, a) first check it is an actual Police officer b) Consider what information is being requested. Your duty is to give enough data to be compliant, you do not have to disclose everything. RM deals with many of these and we have a very good team, well versed in how to support you when dealing with the Police. We take it very seriously and our technical team is ready to assist with any queries you may have. As far as the third parties point goes, although the Police is a third party, it's more like your application providers and other third parties who deal with you. RM Integris works closely with ParentHub and we have contractual relations in place to ensure schools' data is protected. RM insists that ParentHub has security and technical measures in place to prevent breaches. Should a breach occur, RM has unlimited indemnities such that we can claim the full amount of any damages. RM does this because we have high standards and a good reputation; we are not sure if every supplier an education establishment has a contract with covers that in as much detail, offering the same protection. As part of your data mapping exercise, you should consider any instances where you share personal data with 3rd parties and examine how they use, process, and store it. What if they are doing more with the data than was originally contracted or their systems are not as compliant as you would like.
What evidence do we need from external suppliers where we have to share data to ensure they are compliant, how can we be sure?	There's no accreditation for GDPR, it just says there has to be appropriate technical and security methods in place. Unfortunately there are no hard and fast rules so this is where due diligence comes in. There are other accreditations, such as ICO, which has varying levels of compliance but it really depends on what data is being shared, how it's being stored, and where it is. Within the EU everyone will be compliant with the DPA and, from next year, the GDPR. If you are sending data for processing outside of the EU such as America, India, or Australia, ensure there are model clauses in place. Model clauses are a contractual agreement devised by

	the EU ensuring the correct amount of security is given for non-EU organisations such that, even though there are no equivalent laws in their jurisdiction, they are still bound by appropriate measures. Model clauses are quite prescriptive and RM uses them religiously with any organisation that processes data outside of the EEA on our behalf. Suppliers should be able to tell you with which accreditations they comply. RM's wholly owned subsidiary in India performs regular security audits, at any time RM is happy to share full details of the audits that have been performed. Your suppliers should also be able to audit their activities and provide that data.
Where do we stand with apps that ask for access with our G Suite logins or login with Google etc.?	Google has defined their usage of the data they hold on individuals, these are explained in the following links: - https://edu.google.com/trust/ - https://www.google.com/cloud/security/gdpr/