If you're interested in finding out more about how RM can support you with ongoing GDPR compliance, for peace of mind and to ease the workload:

Email: esafety@rm.com
Call: 0808 172 9532
Visit: www.securityineducation.com/data-protection

RM™
Education

RM™
Education

DATA PROTECTION FOR EDUCATION POST GDPR

Email: esafety@rm.com
Call: 0808 172 9532
Visit: www.securityineducation.com/data-protection

Now the GDPR deadline has passed and the dust has settled a little, are you sure your school complies?

You are likely to have undertaken a number of measures as part of your GDPR compliancy project but how can you ensure that as time passes, your establishment stays on track and continues to be compliant?

Whilst the headlines around GDPR focus on large fines, the reality for schools is that the data privacy and security of their pupil's data is more important than the scale of a fine. The consequences of a data breach to a school and children's data are far reaching and it helps to have a trusted advisor by your side to ensure all bases are covered for your peace of mind. Here's how our GDPR experts and tools can support your school with getting and staying compliant.

Discover

- RM can help you discover what data you have on your network and devices as well as in the cloud. Our Data Discovery service will search your network for Personally Identifiable Information and score that data based on the amount of personal data within it. You can search based on certain criteria e.g. health details or name and also see when that data was last accessed to help with your data hygiene.
- RM Unify shows you which applications have access to your data and what data is being shared with them. You get a consistent identity for your users so they only need to remember one username and password, considerably reducing complex and time consuming password management for both users and the IT team.
- If your school has RM Integris you can use the Datashare Management feature to see any additional applications that have access to your MIS data, such as parental communication tools. This can greatly simplify and significantly enhance communication with parents and pupils.
- If you combine these tools with RM SafetyNet you can understand which web-based applications your users are accessing. This enables you to see if they are putting personal or confidential information on non-compliant websites - or in places you weren't aware of - so you can take swift remedial action if necessary.

Manage

- Once you have updated your policies to ensure your users understand where they should keep the data and where they can and can't process that data, you can use RM Unify to whitelist* the cloud-based applications they are permitted to use and store personal data in.
- To classify your data we can help you implement tools such as Microsoft's Azure Information Protection. This allows users to classify their documents based on labels that are agreed with the school. Once the document is labelled, that label stays with that document through its entire lifecycle and you can enforce policies based on the label, keeping you in control and saving you time.

*whitelisting allows you to specify an approved list of software applications that are permitted to be present and active on your computer system.

Enforce a policy that ensures a highly sensitive document about safeguarding cannot be printed, forwarded beyond the recipient or be emailed outside of the school. This puts you in full control of your data and allows you to revoke access to any document at any time should you fear there has been a breach.

Email: esafety@rm.com Call: 0808 172 9532 Visit: www.securityineducation.com/data-protection

Protect

Whilst there are a number of options to help you protect your data and users, there are some key cyber hygiene practices that you should put in place to give you protection over the most common cyber-attacks:

Consider using a mobile device management tool such as Intune to give you the ability to monitor and control devices and the data on them, whilst still giving users flexibility when using devices in school and home.

Next Generation anti-virus and anti-malware protection

RM Recommend Trend Micro's Cloud Security. It not only protects against common and unknown threats such as ransomware, malware and viruses, but also against malicious web links and attachments through its cloud-based anti-spam filter, helping to avoid teaching downtime and costly outcomes.

Don't run as admin

Ensure your users only have the access they really need on devices, by not using admin access. It is common for teacher's devices to not have the same controls or management as their pupil's. However, they are far more likely to contain sensitive data, which if released to the wrong audience is a data breach that is hard to contain, potentially damaging for pupils and staff, as well as negatively impacting the school's reputation.

Whitelisting

Whilst most schools will have whitelisted applications that are installed locally on devices, this is often not the case for cloud-based applications. Use a cloud-based platform such as RM Unify to whitelist cloud-based applications and make it simpler for your users to access them through single sign on.

Identity

It used to be enough to protect the perimeter of your network to ensure your data was safe, but your data may now be outside the perimeter and in the cloud. The one common factor when accessing that data will be your user's identity and it's vital you protect and manage this effectively. Your privileged users should have multi-factor authentication enabled and you need to have a comprehensive on-boarding and offboarding process to ensure they have access to the data they need whilst working at the school but that it is easily revoked once they leave.

Patching

Many recent ransomware attacks could have been prevented through patching of devices. It is essential to have a robust patching routine but sometimes with limited resource it is difficult to keep on top of all your tasks. We can assess your patch state remotely and apply patches for you, saving your IT team time and ensuring your systems are efficient and secure.

Why not take our simple secure, online review to help you understand more about the ongoing GDPR risks?

Get instant tips and advice, plus receive a free personalised report on your own GDPR compliance.
Visit: www.securityineducation.com/data-protection

How RM Unify – intelligent identity and access management – supports GDPR compliance

- Simplify the process of maintaining a centralised identity store for all users, across cloud applications
- Reduce risk through non-composition based password policies and Multi-Factor Authentication
- Understand your potential risk exposure and identify data that a user has access to quickly and accurately
- Build a map of who has access to which services, and automatically remove access based on group membership and role.

Find out more at: **www.rm.com/rmunify**

RM Unify

How RM Integris – our school Management Information System – supports GDPR compliance

- Straightforward information audit and listing
- Greater control over data sharing and third party access, securing your information
- Record, manage and report on parental consent centrally, effectively
- Ensure personal data is kept accurate and up-to-date
- Create a list of all the data you hold in an electronic, transferable document for individual access requests, available at a click of a button
- Delete data when required in accordance with your retention policies, with surety and speed

Find out more at:
www.rmplc.com/gdpr/rm-education/rm-integris

RM Integris

If you're interested in finding out more about how RM can support you with ongoing GDPR compliance, for peace of mind and to ease the workload: www.securityineducation.com/data-protection