Data Protection in schools and colleges: Questions from the Governing Board/Trustees/Directors

This document, produced by SWGfL is designed to support governors/trustees/directors of schools / colleges in the UK with the upcoming Data Protection changes brought about by the EU General Data Protection Regulation or GDPR. Throughout this document the term school / college is used and refers to any UK state-funded educational establishment covered by the Education Act. However, the good practice highlighted in this document is relevant to any educational establishment, whether state-funded or otherwise, but the statutory requirements differ dependent upon the type of school.

This document does not constitute legal advice and should be used in conjunction with your own source of legal advice. No liability will be accepted in respect of use of this advice.

Awareness and communication

Good data protection awareness is underpinned by managers and leaders own awareness of data protection legislation and its impact. However the 'frontline' of good data protection is the staff members handling the data on a regular basis.

Does the school / college ensure that all staff know about their obligations under the data protection legislation and the school / college policy?
Do all users receive regular security and data protection training?

Why this question is important?	As indicated above, the staff members in your school / college are the frontline of data protection. They often collect, store and manipulate personal data in order to be able to fulfil their duties. It's therefore no surprise that staff are a likely cause of a data breach. Not just accidentally, but also maliciously. Whilst a data protection training programme is unlikely to stop malicious breaches, it has the potential to significantly reduce the occurrences of accidental data loss. Data from SWGfL suggests that training staff members about online safety happens in only around 50% of schools and that only 34% of schools have a data protection policy. Not only that, but you should also consider planning to train volunteers or parents that may regularly visit the school.
What to look for?	▪ An audit of staff skills and understanding of data protection. ▪ A training plan that includes all staff and visitors. ▪ Planned training occurs more than once a year. ▪ Evidence that policies are freely and readily available and well communicated (e.g. posters, school / college website, staff handbooks, etc.).
What is good or outstanding practice?	▪ A full range of training topics, including social engineering and phishing, use of cloud technologies and ransomware attacks covered. ▪ Evidence that the training plan adapts to the needs of the users and the school / college. ▪ Role-specific and detailed training for those who process data more regularly. ▪ Data protection training is mandatory for all staff, irrespective of

	experience, role or skill. ▪ Where a user fails, or has difficulty in an area of understanding, the school / college supports the user to understand.
When might you be concerned?	▪ No training needs audit or training plan in place. ▪ No awareness of data protection responsibilities across staff. ▪ Missing records of data protection training and updates

Policies and procedures

The UK Data Protection Act 2018 (when it comes into force) is the legislation that sits alongside the EU General Data Protection Regulation (GDPR). The new legislation will significantly affect and widen individual rights with regards to their own data (or, in the case of a parent / carer, their child's data).

Does the school / college have up-to-date data protection policies in place? Have these been reviewed in the light of the new data protection legislation?

Why this question is important?	Data made available in SWGfL's annual review highlighted that over one third of UK schools do not have a data protection policy. Schools / colleges are statutorily required to demonstrate compliance with the UK Data Protection Act (when it comes into force) and the GDPR. The recommended way to do this is through the creation and ratification of a clear set of data protection policies. Further information can be found in the UK Data Protection Act 2018 (when it comes into force) section 54, subsection 2 and the EU GDPR, Article 5, section 2 page 118.
What to look for?	▪ There are up-to-date data protection policies in place that meet statutory requirements. ▪ There are systematic and regular review of policies, at least on an annual basis. ▪ Pupils / Students, staff, parents and carers are aware of data protection policy and expectations. ▪ Volunteers, contractors and, where relevant, visitors are aware of data protection policy and expectations.
What is good or outstanding practice?	▪ Policies have been developed and informed by wide professional consultation. ▪ Policies are regularly reviewed through wide professional consultation that includes the views of pupils / students and parents. ▪ Evidence of monitoring and evaluation processes to ensure understanding of, and adherence to, policies. ▪ Linked to and a part of other relevant policies.
When might you be concerned?	▪ Missing or not up-to-date data protection policy ▪ Policy is generic and not relevant to the school / college's needs. ▪ No / irregular review of policies, a lack of records management or version control. ▪ Policies exist but are not publicised to the school / college body and / or are not known by staff and pupils.

Information audit and consideration

All schools / colleges process (collect, store and use) personal data about their staff and pupils / students. UK Data Protection legislation requires all schools / colleges to specify what information is held, where it is stored and who has access to it. All controllers (those who manage the processing of personal data) are required to maintain a record of all processing activity including the legal basis under which they are processing this data.

Has the school / college conducted a data audit / mapping exercise to identify what personal data is processed?

Why this question is important?	Schools / colleges are obligated by legislation to ensure that personal data is protected. Knowing what personal data the school / college processes and why is the first step to understanding how it needs protecting. ▪ How is the personal data collected? ▪ Who has access to it? ▪ What data is held? ▪ Where is it held? ▪ When will the data be disposed of? ▪ How will the data be stored and disposed of securely? With cloud storage services and the range of staff that can access personal data taking the first step in auditing is an important start to ensuring compliance with the law. Only once an audit has been defined and performed can personal data be mapped and the appropriate decisions and protections made. Furthermore, planning for and controlling your data sharing mechanisms is a requirement under the new legislation. Wherever a school uses a processor to process information for the school / college, there needs to be a clear contract between both parties. This means that whenever you routinely share personal data there should be a contract defining and controlling this and laying out the manner in which the data from the school / college will be processed and audited.
What to look for?	▪ The school / college is able to identify what and how personal data is collected. ▪ A list of all the storage locations for personal data and what is contained in each location. ▪ A record of processing activity. ▪ Users only have access to the data they need to use and no more. ▪ An up-to-date data retention policy with an associated disposal log.
What is good or outstanding practice?	▪ The record of processing activity includes the lawful basis under which processing activity is taking place and records when and how the data will be (or was) disposed of. ▪ User accounts enable the users to request, or temporarily obtain, access to personal data as necessary to their role. ▪ The audit is reviewed after six months with further actions considered.
When might you be	▪ There is no record of processing activity. ▪ The school / college does not readily know what personal data is processed.

concerned?	▪ The school / college does not know where personal data is stored. ▪ There is no data retention or safe disposal policy

Please note that there are occasions where you MUST share data for example:

In an emergency situation:

For example, a police officer contacts you by telephone as there is a live case of a pupil / student at your school being at risk of immediate harm, they are at risk of suicide. The officer needs to contact their parents and only has limited information to do so. Your school / college name and the name of the child is all they have. They request the parental address and phone number from you.

As this is a true life and death situation sharing the details with the officer is appropriate under the lawful base of vital interest or legitimate interest. Clearly acting in the best interest of the child in this case would mean that sharing the information is the right thing to do. However, it is important to ensure that this is not a fraudulent request and therefore, a reasonable identity check should be carried out to verify that the officer is indeed a current and serving police officer.

Crime and Disorder Act 1998 - Police and other Authorities

Section 115 of this Act allows for the exchange of information to an individual or group where that disclosure is necessary or expedient to support of the local strategy to reduce crime and disorder, the youth justice plan or any other purpose of the act. This act allows disclosure of information (including that which identifies a person) to the police, Local Authorities, Probation services or Health services, where disclosure is necessary. This Act provides agencies with the power to disclose, but does not impose a requirement on them to disclose.

If a request is made under this Act, there should be a defined process available under which a staff member is able to identify what, if any, information should be disclosed. Under GDPR a school / college it is likely that the legitimate interests base would be used to facilitate this disclosure. Please see later detail about legitimate interests.

Children and consent

How does the school / college gather consent for processing personal data, particularly children's data and associated formal parental / carer consent?
Has a record of consent been established?

Why this question is important?	The GDPR provides six lawful bases for processing data. For many schools / colleges the processing of personal data is likely to be performed under the lawful base termed 'public task'. In essence as long as the activity is necessary and the requirement, or task, is laid down in law then you may process the personal data and do not need to look for any other basis. Care should be taken to ensure that the data is not collected for one reason (under public task) and then re-used in another way that does not constitute a public task. For example, a parental / carer address and phone number may be essential for a school / college to process under law, but it would then not be lawful to process this is a different way by, for instance, sharing this with a third party parental communication system used to promote school events and other notices. In this situation another lawful base should be identified and for this, consent is most likely. Consent under the regulation has changed. In the EU GDPR (Article 4 (11)) consent is defined 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;"* This means that where a school / college is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. Pupils / students aged 12 or over may be able to consent to their data being processed. For 'information society services' (e.g. a service over the internet) this is 13 years of age. School / Colleges should satisfy themselves that their consent forms are clear and written in plain English. Consent should also detail in a very clear and specific way why this is necessary, what will happen to the data, and, how and when it will be disposed. Schools/ Colleges should ensure that where consent is being relied upon as the basis for processing personal data that the consent does not lead to an imbalance of power. This means that asking for consent to process personal data when the pupil / student may feel that they have no choice but to consent is not lawful. Consent must be freely given and the pupil / student should not be disadvantaged by their decision not to give consent should this be the case. In some situations, processing of data for non-public task reasons may be undertaken under the 'legitimate interests' base. For example, if consent is withdrawn, but the processing still needs to take place and this is reasonable and with a minimal privacy impact or has a compelling reason, then the school /

	college could use 'legitimate interests'. The ICO provides a 3-part test to help identify whether legitimate interests applies. Another example where legitimate interests may be relevant is in the case of postal marketing material. As long as the school / college can demonstrate the minimal privacy impact, proportionate use of data and that people would not be surprised or likely to object, then using the personal data in this way may be appropriate. For electronic marketing activity the school / college will still require consent under PECR.
What to look for?	▪ Public statements - including who can get access to data. ▪ Clear, established and effective routes for gaining consent from all users, including parents / carers of children under 12 or 13 in the case of 'information society services'. ▪ Clear processes when staff or students register at the school / college and subsequently leave. ▪ Robust and managed records of consent.
What is good or outstanding practice?	▪ Evidence of clear, well-communicated, easy-to-understand notices to all school users on what personal data is collected stored and processed. ▪ Consent is made clear to all staff across the school and as much as practicable to pupils / students in language relevant to their age ▪ Pupils / students actively involved. ▪ Culture of consent - informal and formal (i.e. staff feel confident, talk about in class etc.).
When might you be concerned?	▪ No evidence that informed consent has been sought ▪ Staff and pupils / students have little knowledge of how their data is collected, stored and processed ▪ There are no clear routes for users to obtain relevant access to their personal data.

Responsibility and Assessment

Who is your designated Data Protection Officer? Who is responsible for ensure future data protection compliance including data protection impact assessments?

Has the school / college appointed a Data Protection Officer (DPO)?

Why this question is important?	The requirement to appoint a data protection officer is a statutory requirement under GDPR – Articles 37, 38 and 39. In short you must appoint a DPO if: ▪ You are a 'public authority' – this is highly likely to be the case for state-funded English and Welsh schools. ▪ You carry out large-scale monitoring – such as; attendance, attainment or behaviour records processed either in school or the cloud. ▪ You process large amounts of 'special category' data or criminal convictions or offences (such as DBS checks). The Officer: ▪ Should have expert knowledge of data protection law ▪ May be designated as data protection officer by several organisations ▪ Must publish the contact details of the controller ▪ Must be involved in all data protection matters ▪ Must be provided with all required resources ▪ Must be independent of the controller and not be subject to any conflict of interest ▪ Must report directly to the Headteacher / Governing Body ▪ Must be entrusted with the tasks laid out in section 69, including: advising and monitoring data protection impact assessment procedures, monitoring compliance with policies and monitoring the controller, assigning responsibilities, raising awareness, training, conducting audits.
What to look for?	▪ A clear line of communication between the highest management level of the controller and the appointed DPO, either internally, or as a service from a third party, or consortium / cluster. ▪ Clear evidence that the school has sufficient skills and staff to ensure that personal data is kept safe and secure.
What is good or outstanding practice?	▪ The DPO has a proven history in data protection and has attended a range of training events / courses and has a relevant qualification for example; CISSP, CISMP, PC.dp ▪ The DPO regularly updates their own knowledge. ▪ The DPO is fully resourced and able to directly contact the Headteacher / Governors where a decision is required.
When might you be concerned?	▪ There is no DPO. ▪ The DPO is not able to perform their duties owing to lack of resource. ▪ The DPO does not have suitable experience / qualification. ▪ The DPO is not involved in all issues relating to data protection. ▪ The DPO is influenced, or instructed by senior managers in the performance of their tasks. ▪ The DPO is not independent from direct personal data processing at the school / college ▪ The DPO is not empowered to make decisions independently and / or has been penalised for carrying out their duties.

Personal Data Breach Procedures

What are the school / college procedures in the event of a personal data breach?

Why this question is important?	Strong data protection leadership should lead to a school / college adopting good data protection procedures and policies and that this will reduce the likelihood of a data breach occurring. Nevertheless this eventuality should be planned for. Under the new legislation not all data breaches need to be reported. Where a breach results in a 'risk to the rights and freedoms of natural persons' then this mu should be reported to the ICO within 72 hours of discovery, where feasible. If a breach requires notification owing to a 'high risk to the rights and freedoms of natural persons' then the data subjects shall also be notified, without delay. It follows, therefore, that good data breach notification and business continuity plans should be drawn up to plan for the most likely scenarios. This may be delegated from the Headteacher to the DPO, or the DPO in partnership with other staff/technical support partners. Either way, this process should be clearly documented and made available to those who need access to it. Furthermore, data breach, business continuity and disaster recovery plans should be tested at least annually to verify that the systems and processes would operate as expected in the event of an incident occurring.
What to look for?	▪ A suite of related data breach, disaster recovery and business continuity plans, perhaps drawn together in a single document and / or flowchart. ▪ Evidence of these plans having been tested. ▪ Data protection officer involvement in the production of the policies and procedures. ▪ Effective data backup systems and procedures.
What is good or outstanding practice?	▪ Systems have been tested termly. ▪ There is evidence of a wide range of stakeholder involvement in the planning process ▪ Wider staff members are aware of the policies and understand their role in the event of a situation occurring. ▪ Effective data backup systems and procedures that are regularly tested and include off-site copies.
When might you be concerned?	▪ There are no plans for disaster recovery, breach notification or business continuity.

Appendix One: Where to go for support.

1) Does the school / college ensure that all staff know about their obligations under the data protection legislation and your policy? Do all users receive regular security and data protection training?
    - The ICO's information for Education
    - The ICO's Preparing for the GDPR: 12 steps to take now
    - SWGfL has partnered with DeltaNet to provide online training.
    - What the EU GDPR means in 1 minute from ITGovernance
2) Does the school / college have a suite of up-to-date data protection policies in place? Have these been reviewed in the light of the new data protection legislation?
    - The ICO's information for Education
    - The ICO's Preparing for the GDPR: 12 steps to take now
    - 360data from SWGfL contains legally prepared template policy documents
    - Data from SWGfL suggests that around one third of schools do not have a data protection policy
3) Has the school / college conducted a data audit/mapping exercise to identify what personal data is processed?
    - The ICO's information for Education
    - The ICO's Preparing for the GDPR: 12 steps to take now
    - Iain Bradley from the DfE produced a blog in his role as a governor
    - A video from Ian Bradley from the DfE explaining how to create a data map
4) How does the school / college gather consent for processing personal data, particularly children's data and associated formal parental/carer consent? Has a record of consent been established?
    - The ICO's information for Education
    - The ICO's Preparing for the GDPR: 12 steps to take now
    - This sales piece from Consentua includes some good information about consent
5) Has the school / college appointed a Data Protection Officer (DPO)?
    - The ICO Education FAQs has some useful guidance
    - GDPRinSchools blog helps in making a decision about a DPO
6) What are our procedures in the event of a data loss?
    - The ICO has a guide to personal data breaches
    - Advice from the ICO in the event of a security breach
    - Experian produce an annual data breach response guide
    - Andrew Williams from SWGfL has some advice