GDPR Frequently Asked Questions

Topic/Issue	No.	Question	Response
1. Roles of data controller/data processor/DPO	1.1	What is a Data Controller and a Data Processor?	*Schools are regarded as 'data controllers'. This means that they determine the particular ways, reasons and means in which they utilise the personal data which they hold (primarily relating to their students and staff).* *'Data processors' only use the personal data transferred to them in the particular way that the 'data controller' instructs. Data processors for schools, include the suppliers which process personal data for the school, e.g. relating to transport, finance, or the school text messaging service (they may only use personal data in the way agreed with the data processor).*
	1.2	What is the role of the EA Data Protection Officer for/in schools?	*Under GDPR, schools must appoint a Data Protection Officer (DPO).* *The main role of the DPO is to work with the Principal to ensure the school is complying with GDPR and all other data protection laws. The role involves advising school leadership and staff about their data obligations, monitoring compliance, training, and conducting internal audits.* *The DPO will provide the school with expert advice and guidance on all data protection matters including when data protection impact assessments are required.* *Although the Principal must act as the first point of contact in relation to all data protection matters, the DPO is also accessible.* *The DPO should also be able to report directly to the Board of Governors and be the point of contact for communication with the Information Commissioner on behalf of the school.* *The Education Authority has offered to fulfill this role on behalf of all schools. A school may appoint their own DPO if they wish. In these cases, EA will be seeking assurances from controlled and maintained schools that these arrangements are fit for purpose.*

Topic/Issue	No.	Question	Response
			Schools who have elected the Education Authority as DPO should ensure that they comply with all Education Authority guidelines and requests for information.
	1.3	As Nursery Schools don't have the services of C2k/SIMS are Nursery School Principals data controllers and data processors?	*Please refer to the response at FAQ no. 1.1.* *Nursery schools are data controllers as they hold and determine the ways in which they use data relating to their pupils (e.g. names, parental contact information, medical requirements etc.) as well as data relating to the nursery staff.*
	1.4	Whose role is it to ensure that a school is GDPR compliant? Where does responsibility/accountability lie? Are the Board of Governors ultimately responsible?	*It remains a school's responsibility to comply with the GDPR, acting through its Principal and ultimately the Board of Governors. The Board of Governors and Principals must assure themselves that effective mechanisms are in place to protect personal information.* *The role of the DPO is to support the school with the provision of advice, support material and internal audit.*
	1.5	If a school does not use the EA as DPO, does the EA still have a requirement to provide support to the school?	*If schools are availing of a DPO service outside of EA, it would not be appropriate for the EA DPO to advise and assist those schools. However, there is a range of information and guidance on the EA website which is available for all schools to use as they wish.*
2. Action required by 25th May	2.1	Do privacy notices and a data protection policy need to be in place by 25th May?	*Yes, GDPR was implemented on 25th May 2018.* *If not already been completed, these documents should be created as soon as possible.*
	2.2	What is an Information Asset	*The GDPR legislation requires all data processors to have carried out a*

Topic/Issue	No.	Question	Response
		Register (IAR) and when does the Information Asset Register (IAR) have to be completed for?	*Personal Data Audit. The output of this is the Information Asset Register.* *For schools that have elected the Education Authority as their DPO, if this has not already been completed, then it should be done as soon as possible.* *Schools need to know what data they are holding, where it is stored and how it is currently being processed to understand what needs to be done in order to become GDPR compliant. Schools should keep their IAR updated and under review as a matter of routine.*
	2.3	What do we communicate to parents/legal guardians about GDPR?	*We inform parents and guardians what personal data we collect, how we use this data, third parties involved with this data, and their rights in relation to this data.* *One of the tools you may use is the Privacy Notice, a template which has been uploaded to the Thinkdata website.* *The ICO recommend a layered approach in providing privacy information. They may be provided in a number of different ways. Schools may consider:* • *giving a hard copy of the privacy notice to parents of new pupils ;* • *emailing parents a copy of or link to the notice;* • *making the notice available on the school's website/noticeboard; and* • *referencing the privacy notice in communications with the parents.*

Topic/Issue	No.	Question	Response
3. Policies	3.1	Do schools need to write a policy for managing personal information?	*Yes. In light of the multitude of personal information held by schools (including special categories of personal information), schools will be required to detail how they comply with the enhanced obligations of the GDPR.* *Each school should therefore have a policy for managing personal information (Data Protection Policy), from which the school's Privacy Notice will be derived.* *Templates for these documents are available on the EA website at: www.eani.org.uk/thinkdata*
	3.2	Do schools need to implement a clear desk policy?	*No, a clear desk policy is not a strict requirement of GDPR. However, schools must ensure that personal data is managed and used with integrity, security and confidentiality. Schools should therefore consider their desk policies in relation to their various staff members.* *The Education Authority are aware that operating clear desk policies may not be practical for many classroom settings, however, It is necessary for schools (through policy) to ensure that that no personal data (e.g. reports, letters from parents etc.) are left on their desks or accessible to others when they leave the room.*
	3.3	What aspects of consent have changed with GDPR from original DPA?	*GDPR sets out a number of changes for consent with respect to personal data.* *In relation to consent for data protection:* • *Consent requires a positive opt-in. You can no longer use pre-ticked boxes or any other method of default consent.* • *Explicit consent requires a very clear indication. Implied consent is not valid consent now.* • *Consent requests should be kept separate from other terms and conditions on forms.*

Topic/Issue	No.	Question	Response
			• *Be specific so that you get separate consent for separate things. Vague or blanket consent is not enough.* • *Be clear and concise.* • *Name any third party controllers who will rely on the consent.* • *Make it easy for people to withdraw consent and tell them how.* • *Keep evidence of consent – who, when, how, and what you told people.* • *Keep consent under review, and refresh it if anything changes.* • *Avoid making data processing consent a precondition of a service, e.g. without consent a pupil cannot participate in an event. This will not apply to health and safety and participation waivers, if these are not signed then pupils cannot participate.* *Guidance on Consent is available on the EA Think Data website at: www.eani.org.ik/thinkdata and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/* *Note: the standards in relation to child protection and participation consents remain the same.*
	3.4	What is the difference between a privacy notice and data protection policy?	*A privacy notice is a public document that communicates privacy information to those people about whom you hold personal data. It sets out how you will process their data lawfully and in accordance with the GDPR.* *A data protection policy is an internal document which sets out the processes and procedures your school has adopted in order to ensure compliance with the GDPR in the processing of personal data.*
	3.5	Will C2k be updating their privacy notices for schools also?	*Yes, C2k are currently in the process of finalising a privacy notice which will be accessible for schools through the C2k MySchool portal.*
	3.6	Does it suffice to have a blanket	*No, under the GDPR individuals have the right to be informed about the*

Topic/Issue	No.	Question	Response
		statement in safeguarding and admissions policies regarding information which is shared with third parties?	*collection and use of their personal data. This is a key transparency requirement under the GDPR.* *Please refer to the response to FAQ No. 2.3*
	3.7	Do the data breach procedure, IAR and privacy notice need governor approval?	*Yes. It is recommended that these documents be approved by the Board of Governors*
	3.8	Does a Privacy notice have to be signed by parents?	*No, a privacy notice does not need to be signed by parents. Schools should consider including the privacy notice in the new school year information pack for pupils/parents.*
	3.9	Is it ok for schools to refer to Privacy Notices online or must they be provided in hard copy?	*It is not a requirement of GDPR for Privacy Notices to be provided in hard copy.* *You can publish your Privacy Notices in different ways, for example: on your school website, notice boards or in newsletters. We recommend publishing the Privacy Notice on the school website, where a school has one.* *You must tell people how to access your Privacy Notice. It is important that you review all of the forms used to collect personal data and include how to access your Privacy Notice. For example, this will apply to parental permission forms.* *There are a number of techniques you can use to provide people with privacy information. You can use:* • ***A layered approach** – short notices containing key privacy information that have additional layers of more detailed information.* • ***Dashboards** – preference management tools that inform people how you use their data and allow them to manage what happens with it.*

Topic/Issue	No.	Question	Response
			• ***Just-in-time notices*** *– relevant and focused privacy information delivered at the time you collect individual pieces of information about people.* • ***Icons*** *– small, meaningful, symbols that indicate the existence of a particular type of data processing.* • ***Mobile and smart device functionalities*** *– including pop-ups, voice alerts and mobile device gestures.* *Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.* *Taking a blended approach, using more than one of these techniques, is often the most effective way to provide privacy information.*
	3.10	Where primary or nursery schools provide work placements for young people who are pupils of other post primary/special schools, should their privacy notice include reference to child consent for those over 13 years old?	*Like any adult volunteer with access to personal data, pupils on work placement must be made aware of their work responsibilities in relation to personal data and adhere to the policies of the school and therefore fall within the school's existing staff privacy notice.* *The EA will be revising guidance for schools regarding work experience to include advice on complying with GDPR requirements.*
4. Children's consent	4.1	What is the age of child consent in GDPR context?	*Schools need to consider this question for online and non-online services.* *<u>Online services</u>* *In relation to online services (such as the use of social media or online games or third party interactive learning systems), the age of consent for a child is from 13 years old. If the child is less than 13, or, for whatever reason deemed incapable of giving informed consent, then the consent must be sought from the parent or guardian for the child.* *<u>Non-online services</u>*

Topic/Issue	No.	Question	Response
			GDPR does not set out the general age of child consent for non-online services. Schools must consider the appropriate age for children to be able to consent and in doing so they should consider the age at which children would fully understand their actions and the consequences of giving their consent. Schools may wish to align this age of consent in relation to GDPR, with the other consents sought, e.g. school educational visits consents. *Schools need to document their rationale for electing a particular age for children consent.* *If schools wish to rely upon consent from children, then schools must ensure that the child can understand what they are consenting to, otherwise the consent is not 'informed' and therefore is invalid.*
5. Staff training	5.1	Do all school staff need to be trained in GDPR? Is there a timeframe?	*It is important that all school staff are aware of their responsibilities for the protection of personal information. Schools should take appropriate steps to ensure that all school staff are suitably trained on GDPR.* *To support schools, EA has provided online GDPR training for the principal and one other member of school staff. This should be completed as soon as possible. EA is working on extending these training arrangements as an option for schools to use for further staff training.* *There is a range of materials available on the EA and ICO websites to assist schools in raising awareness of GDPR and the safe handling of personal information.*
	5.2	Will EA keep records of each school's completion of the online GDPR training?	*Partially, the Education Authority keeps a record of all the ELearning which has been requested and completed by a school. Each school is currently entitled to 2 places on the E-Learning 'GDPR Governance' programme.* *The Education Authority does not keep a detailed record of attendance at*

Topic/Issue	No.	Question	Response
			information sessions run or small group sessions. It does not keep a record of training materials downloaded by a school for internal training. Schools are advised to keep these records themselves.
6. Access/Security of data	6.1	Is there an issue regarding the extent to which secretarial staff have access to information?	*Administrative/secretarial staff in schools have access to personal data as part of their job and therefore schools need to ensure that they comply with the GDPR principles.* *The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process that data unless you have instructed them to do so and there may be an issue regarding the extent to which secretarial staff have access to information. It is therefore vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.* *You should provide appropriate initial and refresher training, including:* • *your responsibilities as a data controller under the GDPR;* • *staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;* • *the proper procedures to identify callers;* • *the dangers of people trying to obtain personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognize 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and* • *any restrictions you place on the personal use of your systems by staff (e.g. to avoid virus infection or spam).* *Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable* *Schools should restrict all staff access only to the information that they need in relation to their role.*

Topic/Issue	No.	Question	Response
	6.2	If a school rents out accommodation to external agencies/community groups, do the children's books need to be locked away?	*This depends, in part, upon whether the external agency / community group will be using classrooms or whether it will only be in a communal space where children's books and materials etc. aren't stored e.g. sports hall, assembly hall.* *To the extent that an external agency / community group is using a classroom, it would be recommended to lock away children's work, if possible, with the exception of public displays of children's work.* *Names on children's work amount to personal data and the contents of children's work may make it possible to draw conclusions regarding a child's academic performance. Schools should therefore ensure that children's work, is stored out of sight or if possible locked away before a third party uses the classroom.* *It is likely that personal data would be stored in other ways in a classroom too e.g. copies of pupil progress reports, SEN/child protection documents, etc. Such sensitive personal information should as a matter of course be stored securely at all times.* *If children's work is not going to be locked away before an external agency / community group uses a classroom, that agency / group will be deemed to be a data processor of the children's personal data under GDPR (by virtue of having access to the classroom and the personal data stored therein). The school must therefore enter into a data processing agreement with the third party agency / group.*
	6.3	How do schools manage data access with short term temporary members of staff, e.g. substitute teachers/classroom assistants?	*Short term temporary members of staff are required to comply with GDPR in the same way as permanent long-term staff. As for permanent staff, temporary staff should be aware of what personal data is, what 'processing' means and what their duties are in handling personal data.*

Topic/Issue	No.	Question	Response
			The access to personal data given to short term staff should be no more than to the extent necessary e.g. a temporary teacher will need to know details of any health / educational needs affecting the children in their class(es) and would also need to know of serious health issues affecting children in the school generally e.g. nut allergies, but would not necessarily need SEN details of children in other classes in the school.
	6.4	Is it ok to scan letters, written reports, etc. and upload pupil information such as SEN information to SIMS or school file servers?	*SIMS continues to provide a protected environment where schools choose to upload documentation there. However, schools should be aware that when using printers/scanners there may be a small risk of information being retained in the memory of those devices.*
	6.5	Should schools send data capture forms home to parents using recorded delivery?	*As data capture forms contain personal data, they should be circulated securely and due to the sensitive nature of details contained within these forms they should be treated with particular care. The Education Authority recommends that data capture forms may be sent by non-recorded post.* *They should not be sent home in children's school bags.*
	6.6	Where schools require back up paper copies of personal information, such as contact details for pupils, how should this be managed?	*This is up to the schools to decide. The ICO advises data controllers such as schools to consider risk analysis, organisational policies and physical and technical measures when considering security arrangements for personal data.* *Note that several GDPR principles relates to limiting storage. Personal data should not be retained for longer than necessary in relation to the purpose for which such data is processed.* *Personal Data (even paper records) must be stored in such a way that the data can be disposed of reliably when it is no longer required. Note that any personal data kept by a school must be managed in accordance with the Department of Education Model Disposal of Records*

Topic/Issue	No.	Question	Response
			Schedule: https://www.education-ni.gov.uk/publications/disposal-records-schedule *Finally, GDPR requires that ALL personal data is held securely.*
	6.7	Where there is insufficient lockable storage for personal data, should office doors be kept locked, e.g. secretary's office?	*The GDPR requires that personal data be processed securely by means of 'appropriate technical and organisational measures.' A risk based approach in line with 6.6 above should be undertaken to identify how best schools should maintain the security of personal information.* *Where there is currently insufficient lockable storage for personal data, steps ought to be taken to rectify this.*
	6.8	If schools are sharing data with e.g. DE (census data), FFT, etc. is there assurance that those organisations are also GDPR compliant?	*The services supplied to schools by C2K (EA) are undertaken on behalf of the Minister and the Department. Data sharing in this environment is compliant with GDPR. DE is the data controller for school census data and it is their responsibility to ensure GDPR compliance in this regard. Data sharing is allowed with a number of other agencies, including Fisher Family Trust through C2k's contract with their main service provider, Capita. The contract with Capita has been updated in-line with GDPR and this cascades down to the subcontractors.* *If schools are sharing data with any other commercial third party (e.g. their suppliers), a data processing agreement should be put in place. This may form part of a contract between the school and the third party, and should be reviewed regularly. The ICO has provided guidance as to what a data processing agreement should document. EA is designing guidance in this area.* *The sharing of data agreements between schools and other public bodies is currently under review.*

Topic/Issue	No.	Question	Response
	6.9	Where external organisations/agencies use school accommodation (e.g. HSCT service) who is responsible for data management within those services?	*This depends upon the nature of the services provided.* *If the services are provided and initiated by for example, HSCT, the HSCT are responsible for the personal data.* *However, if the services are administered as a joint project, the school and for example, HSCT will be jointly responsible as data controllers and a joint controller agreement should be put in place. An assessment of whether the body providing the services is a data controller is required.* *Please also refer to the response to FAQ No. 6.2*
	6.10	Where schools are organising educational visits and teachers will be responsible for pupils' passports, medical records, contact details, etc. is consent required or do parents need to be informed?	*Consent for the actual activity remains as usual. GDPR is only concerned with processing personal information.* *In relation to GDPR and the holding of passports, student information, medical conditions etc. by staff, consent is not required. Teachers will already be holding much of this information in relation to their pupils whilst at school, and they have legal grounds for doing so whilst on educational visits. Teachers must ensure that this data is handled securely at all times whilst on educational visits. Data held MUST be recorded in the information Asset Register.* *Schools should outline within their privacy notice that pupil's personal information may be carried by school staff when on school educational visits.*
	6.11	Many primary schools struggle to have secure storage space to file the large individual pupil records for the required period – can you	*In an effort to increase efficiency and future proof the school's systems, schools may consider switching to electronic records by scanning documents.* *Schools may consider using secure off-site storage providers to safely secure*

Topic/Issue	No.	Question	Response
		advise how this might be managed?	*records that do not necessarily need to be onsite (perhaps records that urgent access would not be required) but which cannot be destroyed. Schools must be satisfied that the information will be held securely.* *It is also incumbent upon schools to remove data which is no longer required.*
	6.12	Is it ok to store personal data on a portable hard drive if password protected?	*Yes, however it is vital that personal data on portable devices is encrypted and password protected. Portable devices are easily forgotten, mislaid or stolen and in such an event where the device is not password protected then that amounts to a data breach which may be reportable. Even encrypted devices might require reporting to the ICO, depending upon the consideration of the school DPO.* *There is a very real risk of reputational damage by losing portable devices.* *There should be a policy on the use of such devices in any event.*
	6.13	Given that C2k is accessible from personal mobile phones, what should be the policy re access to/storage of personal data for teaching staff?	*Mobile devices such as phones are very vulnerable to breaches because they are by far the most lost or stolen devices and generally have much weaker security.* *The following policies should be adapted:* • *denying or restricting access to sensitive data on devices which lack a high level of encryption;* • *auditing the types of personal data being processed and the devices used to access that data;* • *controlling access to data and/or devices using passwords or PIN codes;* • *backing up copies of data held on mobile devices.* *DE guidance on the deployment of mobile ICT can be found in DE Circular 2016/26 Effective Educational Uses of Mobile Digital Devices accessible at: https://www.education-ni.gov.uk/publications/circular-201626-effective-*

Topic/Issue	No.	Question	Response
			educational-uses-mobile-digital-devices
7. Pupil Progress Reports	7.1	How should pupil progress reports be shared with parents?	*Pupil progress reports include personal information relating to pupils. Schools must take reasonable measures to safeguard this information. Pupil progress reports should be distributed in a way that ensures that the information is secure.* *Schools should consider the following methods for sending reports to parents/guardians:* *- by post;* *-by email where email addresses have been confirmed; or* *- by uploading to the school's secure access VLE.* *Sending Pupil Progress Reports home in schoolbags is not recommended.*
8. Archived/historical data	8.1	Where schools have photos on wall displays with pupil/past pupil names, should these now be removed?	*Where schools hold and display historic photographs, the Education Authority would recommend the following:* *(i) Schools may display historic photographs of student groups, sporting teams, head boys/girls on the grounds that this is both in the general public interest and is in the schools' 'Legitimate Interest' of promoting itself.* *(ii) Schools may wish to use historic photographs in advertising material, alumnae events or historical records. The Education Authority would recommend that photographs within such publications be published only with a generic description (e.g. class of 1980 or 1st XV Rugby team 1999) and without individual student names so as to protect the individuals' rights.* *However, it should be considered that data protection laws do not apply to the deceased and therefore, very historic photographs (e.g. from 1800s) may be used whatever way the school sees fit.*

Topic/Issue	No.	Question	Response
	8.2	How should schools manage archiving of information e.g. for anniversary events?	*Schools should only retain personal data for as long as necessary and in accordance with the retention periods. Once the retention periods have lapsed, the information should be securely destroyed.* *If schools wish to keep certain historical data for anniversary events (pictures, year group names and particularly notable achievements) the school can retain such information as it is in the schools' 'Legitimate Interest' of promoting the school. However, the information should only be that which acts to achieve such 'Legitimate Interest' and nothing else, e.g. sports' photos and year group records would likely be acceptable, but specific behaviour reports or progress reports are not likely be acceptable in this regard.* *Again, it should be considered that data protection laws do not apply to the deceased and therefore, very historic information (e.g. from 1800s) may be used whatever way the school sees fit.*
	8.3	What do schools do with existing archived information, e.g. old school registers, school/pupil reports?	*Schools should only retain personal data for as long as necessary and in accordance with the relevant retention periods.* *However, it should be considered that data protection laws do not apply to the deceased and therefore, very historic photographs (e.g. from 1800s) may be used whatever way the school sees fit. Schools may wish to retain this data for historical purposes.* *Please refer to the response for FAQ No. 8.2*
	8.4	Where a school wishes to keep photographs of school sporting/drama events does this need to be noted on IAR and in	*Please refer to the responses for FAQ Nos. 8.1 and 9.1.* *Yes, schools should reference school photographs in both its IAR and privacy notice.*

Topic/Issue	No.	Question	Response
		privacy notice?	*If schools wish to display named photographs of students, explicit consent must be acquired. Note that individuals may wish to withdraw consent at any time.*
9. Pupil Photographs	9.1	Is consent required for use of pupil photographs?	*Consent is required for the use of pupil photographs in certain circumstances.* *If a school wishes to use pupil photographs for general display or publication purposes, parental consent should be sought regularly. The frequency should also be stated in the school's pupil and parent privacy notice.* *Where pupil photographs are used for identification purposes within the secured pupil records, e.g. on SIMS, consent is not required. A school may consider using public task as a legal basis for processing in using the pupil photographs for this purpose and therefore consent is not required.*
	9.2	Is consent required retrospectively or only for future use of photographs?	*Consent should be sought for the future use of photographs for publication or general display.*
	9.3	Can consent for use of pupil photographs be asked for with no indication of retention/disposal dates?	*When seeking consent, schools should make sure that they clearly specify the time period for which the photographs will be retained. This should be no longer than is necessary.* *Anonymous photographs do not usually constitute personal data. Remember that consent may also be removed, and the subject may wish to exercise destruction rights also. These have to be managed in a sensitive way, and for as long as the retention is planned for.* *Retention of all documents is currently under consideration and further*

Topic/Issue	No.	Question	Response
			guidance will be issued in due course.
	9.4	Do you have to delete pupils' photographs from school website at end of each year?	*Schools do not need to delete photographs from the school website each year provided that they have consent in place to use the photographs for this purpose and have set out the length of retention within such consent.* *Schools only need to stop using these photos once the time period for retention has lapsed.* *Please refer to the response for FAQ No. 9.3*
	9.5	Should schools allow third parties to take pupil photos, e.g. at sporting/drama events or should schools have a no photography policy?	*This is a matter for each individual school's Board of Governors. There is no requirement that schools adopt a no photography policy at sports, music or drama events from a GDPR perspective. Data protection does not apply to the use of personal data for personal or household activities.* *From a protection principle, schools may wish to have clear guidance regarding parent/others taking photographs and videos with respect to school social media policies, e.g. parents may not post photos/videos of school events which include children other than their own on social media sites. Where a school event includes children for whom consent to take photographs/videos has not been provided, the school must decide how to manage this.* *The school would require consent if it wished to photograph the event itself for promotional or other such reasons.* *Guidance has been provided by the ICO at https://ico.org.uk/your-data-matters/schools/photos/*
10. Pupils with medical needs	10.1	Is consent from parents/legal guardians required for display of	*No. A Risk based assessment needs to be made, and the thinking recorded within the IAR. In some schools, a considerable percentage of a class may*

Topic/Issue	No.	Question	Response
		child's photo with medical needs where required?	*have inhalers/eppipens or other emergency medical interventions. It is necessary to ensure the correct intervention is administered to the child.* *The decision to use photographs for the identification of children at risk of requiring urgent medical intervention is ultimately a decision for the school. They must consider a number of factors, such as: the number of staff; the number of children with conditions; risks associated with misapplied medical interventions; the decision to have photographs displayed in at risk (e.g. canteens) areas or staff rooms. A school may consider this necessary as part of its duty of care to pupils (a legal obligation). As this is special category information, schools may consider that the processing is necessary for the purposes of occupational medicine or health care treatment.* *Schools should also inform affected parents/guardians that this is being done. This use must be properly described within the IAR.* *It may be appropriate to have some method of suppressing the pictures when the school is closed e.g. a curtain – to prevent casual access through windows or where the school spaces are being used at night.*
	10.2	Does this need to be sought annually or can it be done on entry to the school for the period of the child's attendance at the school?	*As pupils' social, medical and developmental circumstances may change throughout their school lives, it is recommended that schools refresh these consents on a regular basis as this will act to ensure that the information is accurate and limited to what is necessary.* *This may align with the process of annual review for children whose medical needs are such that an individual care plan is required.*
	10.3	Can schools continue to request that children sign into medical room including provision of parental contact numbers?	*Yes, schools can continue to request that children sign into the medical room and provide parental contact numbers (although these may already be available on the system) as they have a duty to safeguard the child and provide medical care if necessary.*

Topic/Issue	No.	Question	Response
			However, it is recommended that each sign in sheet is independent (rather than a sign in table) and does not contain any other pupil's information (including their signature). It is important that this is not accessible to any other students and once signed is stored securely, for example in a locked filing cabinet.
11. Sharing information with other schools/ Transition information	11.1	Is consent required where schools transfer pupil information to other schools, particularly at transition points?	*Consent is not required for schools to share pupil information with another school to which a pupil is transferring. Schools have a legal basis for sharing this information without consent due to their statutory function to provide a continuity of educational experience, being within their public task.* *The information shared should not be excessive and should only include that which is reasonably required to facilitate an effective transition to the new school, e.g. examination results, name, address, date of birth, special dietary needs, allergies etc.* *It is recommended that if schools are required to transfer excessive pupil information (information which does not facilitate an effective transition to the new school) , that this only be done if consent has been obtained from the parent/carer or alternatively be given to the pupil's parent/carer for forwarding to the new school* *It is important that schools continue to support pupils' transition to other schools in the context of best practice guidance available.* *Nursery Schools/Units and Reception classes in Primary Schools should refer to advice on transition provided in CCEA's 'Curricular Guidance for Pre-School Education' and DE's 'Guidance on Induction and Transition in Pre-School Education and Year One'.* *Primary and Post Primary Schools should refer to advice provided in CCEA's 'Key Stage 2 to Key Stage 3 Transition Guidance: School Collaboration*

Topic/Issue	No.	Question	Response
			Sharing Information to Support Transition in Learning' and the EA's 'KS2/3 Transition Project for Literacy and Numeracy'. *Schools should also note the relevant statutory orders:* - *Department of Education in Northern Ireland (DENI) Post-primary Transfer Policy (2013a) www.deni.gov.uk* - *Department of Education in Northern Ireland (DENI) The Procedure for Transfer from Primary to Post-primary Education Circular 2013/20 (2013b) www.deni.gov.uk* *With reference to transfer of child protection information, specific information is provided in DE Circular 2016/20 Child Protection: Record Keeping In Schools and DE 2017/04 Safeguarding and Child protection: A Guide for Schools.*
	11.2	How do schools respond if such data is requested regarding an individual pupil where there are special circumstances?	*Please refer to the response for FAQ No. 11.1* *The information shared should not be excessive and should only include that which is reasonably required to facilitate an effective transition to the new school, e.g. examination results, name, address, date of birth, special dietary needs, allergies etc.* *It is recommended that if schools are requested to transfer excessive pupil information (information which does not facilitate an effective transition to the new school), that this only be done if consent has been obtained from the parent/carer or alternatively be given to the pupil's parent/carer for forwarding to the new school.* *Direct requests from the school do not have to be complied with – beyond that identified in the circulars in 11.1*
12. Sharing pupil data with commercial suppliers	12.1	Do schools need to check with suppliers regarding data storage e.g texting system?	*Yes, this is important and a GDPR requirement. Schools should check the privacy notices of third party companies with whom they share personal data.*

Topic/Issue	No.	Question	Response
			Schools should also ensure that they have contracts in place with the suppliers who provide these services and that these contracts contain appropriate data processing clauses as required by GDPR. *The Education Authority is currently working on template data processing provisions which schools can provide to existing suppliers and use as a guide for new supplier contracts. These will be published in due course.*
	12.2	Can schools use text messaging service to publicise local community events or do they need to seek consent that numbers may be used for this purpose?	*Yes, however the consent of each recipient is required in order to do so. This can be acquired at the beginning of the year* *There are risks with such services in that they can reveal the personal data of others – a Whatsapp group for example will display everyone's picture (if one is uploaded) and mobile number – so the school must ensure that each user's details are protected.*
	12.3	Do you need to get consent for sharing of pupil data with external organisations such as exam/assessment providers?	*In certain circumstances consent is required.* *In relation to official exam / qualifications bodies (e.g. GCSE or A Level), consent will not be required as the school is carrying out its 'public task' when processing the data in this way, by providing the student with access to e.g. GCSE examinations. However, schools must only provide that information which is required to provide the examination service.* *Consent must be sought before transferring student personal data to third parties for services not set out in law as part of a schools 'public task', e.g. to a driving safely awareness charity who attends the school to deliver a seminar.*
	12.4	Do you need to get assurance of security from school website	*Yes- if the web site contains personal information. GDPR does not concern itself with systems where there is no personal information held. Please refer*

Topic/Issue	No.	Question	Response
		provider?	*to the response at FAQ No. 12.1*
	12.5	If a contractor informs a school that they are GDPR compliant, should the school accept this without further verification?	*No. The Regulation makes it clear that organisations such as schools can be held accountable for breach of the Regulation by third parties, including contractors.* *You need to carry out your own checks of the contractors' processes, to include a review of their privacy notices, to ensure that they comply with GDPR.* *You may require data sharing agreements or modified supply contracts to continue to use their services. EA is working to supply standard versions. It is essential that such things as breach notification procedures are provided to you as a customer.* *You should also ensure that any contractors and third parties they may use are located in the EU and that they will not be transferring data outside the EU.* *If data is to be transferred outside the EU extra care needs to be taken to ensure that an adequate level of data protection is in place in relation to the country to which the information is being transferred, and in the first instance, you should consult your DPO.*
13. Sharing pupil data with other government agencies	13.1	If asked for pupil data by other government agencies such as health or electoral office, do pupils/parents need to give consent?	*Not usually. There may be another basis for processing the information without the need for consent. You will need to consider each situation and the type of information to be provided to those agencies. For example, is there a legal obligation on the school to provide the information to the health and electoral offices? Is the information necessary and in the public interest? Is it in the vital interests of that child for the information to be provided? Vital interests refer only to the saving of a life and would happen only in extreme conditions.*

Topic/Issue	No.	Question	Response
			If the answer to any of these questions is yes, then the information can be provided without consent being required. It is important however that the information provided is not excessive and only comprises information which is reasonably required. *Further, if the pupil information to be provided contains special category data, such as data relating to health or religion etc., schools need to identify not only a lawful basis for processing the information, but also further conditions need to be satisfied.* *Quite often there is a link between the legal basis for providing the information and the additional criteria which needs to be satisfied for processing special category data. For example, if the information is being provided on a public interest basis or to enable a school to fulfil their official function quite often the condition of processing of special category data is also necessary by reason of a public interest criteria.* *Where schools are required to respond to requests from the PSNI related to criminal investigations, Form 81 for disclosure is still required to be completed.*
	13.2	Can the EA provide advice on the process of completing UNOCINI information to share with HSSTs where sensitive parental information is required without having informed parents that the information is being shared?	*Where schools have particular concerns regarding consent within the UNOCINI framework, they should refer to guidance provided by the Safeguarding Board for NI, available at:* http://www.proceduresonline.com/sbni/p_respond_abuse_neg.html *Should more specific advice be required, schools are advised to contact the EA's Child Protection Support Service.*
	13.3	Where EA services or HSCTs	*Special care should be taken when distributing information relating to a*

Topic/Issue	No.	Question	Response
		request information about a child by email, is it permissible to respond by email? Does it need to be encrypted?	*child. It is recommended that sensitive personal information about a child sent by e-mail should be password protected or encrypted and that the recipient's e-mail address should be confirmed in advance.*
14. Visitor Books	14.1	How should schools manage visitor sign-in books and how long should this information be retained?	*As visitor sign in books contain some personal data, these must be treated in a secure manner. Visitors should not be granted access to the personal data of previous visitors and it is therefore recommended that these books are kept closed, stored securely when not in use and each previous entry is hidden* *Schools may also consider adopting a single page approach for each visitor rather than a sign in book. This would involve each visitor signing an individual page and not having access to previous pages.* *Schools should ensure that they signpost visitors to their privacy policy, perhaps with a hyperlink on the sign in page or visitor badge.* *As per the Department of Education guidance these records should be kept for 6 years, after which point they should be destroyed.*
15. Employment Records	15.1	Can a principal keep a file detailing staff absences?	*Yes, as all employers are required to record staff attendance to enable staff to be paid and to manage staff attendance but principals should use the documented process for the school.* *Staff should be informed that it is done through the school's privacy notice.*
	15.2	Do you need staff consent, or to inform staff, when submitting staff employment information to NILGOSC/pension providers?	*No, as employers have a contractual duty to pay their staff a pension, consent is not required to submit information to the pension providers (provided that such information solely relates to the provision of the pension scheme, e.g. employee payment information, salary etc., and not irrelevant information, e.g. disciplinary proceedings)*

Topic/Issue	No.	Question	Response
			Schools should make sure that they list this type of processing on their employee privacy notice.
16. Minute taking	16.1	Should governor minutes include individual names, e.g. when reporting on a staff request for career break or a long term staff absence requiring recruitment of temporary replacement?	*Governor minutes should not generally include names of individuals. This issue will be included in future governor training programmes.* *Where personal information is being recorded (committee papers, for example) – consider encrypted documents.* *All minutes and reports should only be retained in accordance with the Department of Education's Model Disposal Records Schedule: https://www.education-ni.gov.uk/publications/disposal-records-schedule.*
	16.2	Can governor reports be emailed to governor personal emails? Should governor reports be encrypted if sent by email? What if reports include sensitive personal data?	*Governor reports can be sent to governors' personal email addresses and do not need to be encrypted if they do not contain personal information about pupils or staff. Care should be taken to ensure that the information is being sent to the correct email address. As schools must ensure that personal data is secure and confidential, schools may decide to encrypt these reports as an additional security measure to evidence compliance with GDPR.* *Governors must be reminded of their duties of confidentiality as data controllers. They should not store these reports on their personal computers without the appropriate password protections, or should not leave hard copies of these reports unprotected. The Education Authority recommends that Governors keep these school documents password protected or in a locked cabinet when not being used.*
17. Electronic records: staff access	17.1	Can school staff email school information to their own email address so that it may be accessed at home?	*Due to the security provided by C2K it is recommended that staff use C2k email addresses to email sensitive documents– the C2K file management system is also recommended for transfers from work to home. EA recommends that schools should avoid use of USB Sticks for school records*

Topic/Issue	No.	Question	Response
			which contain personal data, however, should schools decide to continue use of USB sticks, they should encrypted and have a policy on their use.
18. Retention and Disposal	18.1	If schools currently hold pupil exam data for more than 6 years, should it be destroyed by 25th May?	*Please refer to the response at FAQ No. 8.3*
	18.2	In nursery schools, do all pupil records need to be retained until pupil is 23 including detailed observational records, or just summative records?	*Nursery schools do not need to keep all personal data relating to their pupils. It is unnecessary for observational reports and other personal data records to be kept once the pupil leaves the school. The Education Authority recommends that summative pupil progress reports including end of year transition reports are kept pursuant to the Department of Education's Model Disposal Records Schedule:* *https://www.education-ni.gov.uk/publications/disposal-records-schedule* *In particular, refer to Section 5 at the above link which is a schedule outlining minimum retention periods and action to be taken after retention. All other personal data can be given to parents or securely destroyed.* *Please note longer retention periods are required for SEN and Child Protection records as per DE's Schedule'*
	18.3	Will SIMS be aligned in the future with data retention timescales?	*Yes, work on this is ongoing. More information on this functionality will be released closer to the time.*
	18.4	Do schools have to keep records of when specific data is disposed of?	*Again, please refer to the Department of Education's Model Disposal Records Schedule:* *https://www.education-ni.gov.uk/publications/disposal-records-schedule* *Section 2 paragraph 3 confirms that a record must be maintained of files*

Topic/Issue	No.	Question	Response
			that have been destroyed.
19. Data breaches	19.1	Can you provide examples of what constitutes a 'serious data breach'?	*Please refer to the ICO guidance on data breaches: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/* ***ANY DATA BREACH – OR SUSPECTED DATA BREACH MUST BE RECORDED AND REPORTED TO YOUR DPO- There must be no exceptions.*** *A serious breach is a breach that interferes with the rights and freedoms of the data subject. A breach will need to be considered having regard to all of the circumstances.* *Listed below are examples of personal data breaches.* • *access by an unauthorised third party – being hacked.* • *deliberate or accidental action (or inaction) by a controller or processor - accidental posting of personal details online.* • *sending personal data to an incorrect recipient – emails and attachments sent to the wrong person.* • *computing devices containing personal data being lost or stolen i.e. USB, iPad, Laptops.* • *alteration of personal data without permission; and* • *loss of availability of personal data – accidentally deleting data/moving it such that it is not recoverable.* *Whether any such personal data breach will constitute a serious data breach will depend upon a number of factors, as follows:* • *The potential detriment to data subjects: - identity theft;* • *The volume of personal data lost, released or corrupted;* • *The sensitivity of the data lost, released or corrupted.*

Topic/Issue	No.	Question	Response
	19.2	When does a breach have to be reported to the ICO? Does a school or the EA's DPO report a data breach to the ICO?	*Certain types of personal data breach must be reported to the ICO within 72 hours of the organisation becoming aware of the breach. The DPO will decide whether to report this to the ICO. Please refer to Q 19.1.* *There is also an obligation to notify the individual (data subject) without delay, **if** the breach is likely to result in a high risk of adversely affecting the rights and freedoms of that individual.* *The Education Authority's DPO will act as a contact point for the ICO, including reporting data breaches.* *Best practice dictates that you keep a record of any personal data breaches, regardless of whether you are required to notify the ICO.* *The Education Authority will issue a Data Breach Management Policy on the ThinkData section of the EA website in due course.*
	19.3	Is teacher leaving parental letters on desk a data breach?	*Of itself, this act is not a data breach, but it does have the potential to become one.* *Please see the response to FAQ no. 3.2.* *Best practice would be for teachers to place such letters into a locked drawer.* *A clear desk policy is not a mandatory requirement but would minimise the risk of a data breach through loss of data or inappropriate access by pupils/parents.* *It is important to note that:* *1. a data controller has the obligation to treat personal data securely; and*

Topic/Issue	No.	Question	Response
			2. a personal data breach does not arise only as a result of loss or theft of personal data but is any breach that interferes with the rights and freedoms of the data subject (including unlawful destruction, loss, alteration, unauthorised disclosure of, or access). *Where possible, classroom doors should be locked when the room is not in use.*
	19.4	When does a data breach have to be reported to ICO rather than reported to BoG and recorded only within the school?	*The decision to report will be made as a collaboration between the Principal and the school's DPO All data breaches should be recorded within the school, and may be reported to Board of Governors. The school's DPO may report to the BOG – depending upon the nature of the event.*
	19.5	Who is liable in controlled schools where there is a fine or compensation claim for a data breach?	*As data controllers, schools will be liable for data protection fines or compensation awards, acting through their Board of Governors.*
	19.6	If a pupil shares data about other pupils on mobile phones within school is that considered a data breach?	*This would only be regarded as a data breach if the pupil obtains the information from the school (e.g. by reading it off a teacher's desk or seeing it on the walls of the staff room) and the school was acting as controller for that information, e.g. medical information, pupil progress reports, family issues, examination results etc.* *This is not a data breach if the pupil receives the data from the other pupil himself or is obtained solely from interaction with other pupils.* *Schools should ensure that they have a mobile phone policy in place.* *Schools should be aware of DE Circular 2016/26 Effective Educational Uses of Mobile Digital Devices* *accessible at:*

Topic/Issue	No.	Question	Response
			https://www.education-ni.gov.uk/publications/circular-201626-effective-educational-uses-mobile-digital-devices
	19.7	Is it a data breach to display individual pupil photographs with medical needs in staff room/office?	*Please refer to the response to FAQ no. 10.1.*
	19.8	If schools receive data in error, is it the responsibility of the receiver to inform the sender? Should the school report this as a data breach?	*If schools receive data in error it is recommended that the school informs the sender and the sender's DPO, and either destroys or returns the data as per their request. It is incumbent upon the sender to report as a data breach.*
20. Subject Access Requests	20.1	Will there be opportunity to recoup cost for Subject Access Requests where excessive time is required to collate the data?	*Where requests are completely unfounded or excessive, in particular due to a repetitive pattern of requests, schools may charge a reasonable fee taking into account the administrative costs of providing information, or refuse to act on the request.* *YOU SHOULD NOT REFUSE A REQUEST WITHOUT DISCUSSING WITH YOUR DPO.* *Schools are only required to supply a single copy of information held; if additional copies are requested, schools can charge a reasonable fee based on administrative costs. Further ICO regulations may be implemented capping fees that can be charged.*
	20.2	If more time is required to collate the data requested in a SAR, can an extension be requested?	*Usually schools must provide the information requested within one month of receiving the request. This period can be extended by 2 further months where necessary, if the request is very complex or the requester has made a large number of requests. This is by exception and should be done in consultation with your DPO*

Topic/Issue	No.	Question	Response
			Schools must inform the requester of any such delay within 1 month of receipt of the request, together with reasons for the delay. *Further Education Authority guidance to follow in relation to holiday periods.*
	20.3	Is there a vexatious clause for SARs?	*Please refer to the response at FAQ No. 20.1*
21. CCTV	21.1	What is the advice for schools who use CCTV cameras?	*The ICO provides a CCTV Code of Practice which is available at www.ico.org.uk.* *The Education Authority would recommend that schools consider conducting a privacy impact assessment taking into account the benefits and risks of CCTV; decide whether they can justify the use of CCTV e.g. it may be in the 'Legitimate Interest' of the school to safeguard pupils and staff, and enhance security; consider if those aims could be met by any other less intrusive means; and think of what steps could be taken to minimise privacy risks e.g. think carefully about the location of cameras.* *There must be clear notices telling individuals that CCTV recording is in progress, and who to contact if any queries arise. The use of CCTV should also be covered in privacy notices issued by the school.* *Remember that subject access requests (SARs) can be made requesting CCTV footage, and the usual process for assessing such a request should be followed. Care should be taken not to inappropriately disclose images of third parties without legal justification.*
	21.2	Can EA advise how these records could be safely stored electronically?	*CCTV footage must not be retained indefinitely. There is no prescriptive time period which must be applied, however, schools must be able to justify that the retention period they decide upon is necessary.*

Topic/Issue	No.	Question	Response
			Only authorised individuals must have access to view footage for justifiable reasons. Footage should be encrypted and access password protected.
22. Social Media	22.1	How do schools manage use of Facebook?	*It is the responsibility of each school to create their own online safety policies, acceptable use policies, etc.* *C2k requires principals to sign up to this on document EN074 accessible to schools through the link below:* *https://www.c2kexchange.net/documentcentre/Documents/EN074%20-%20Acceptable%20Use%20Policy%20for%20C2k%20Services.pdf* *Schools may also refer to:* *https://www.education-ni.gov.uk/articles/internet-and-wifi-guidance* *DE Circular 2016/27 Online Safety:* *https://www.education-ni.gov.uk/publications/circular-201627-online-safety* *DE Circular 2007/01 Acceptable use of the internet in schools:* *https://www.education-ni.gov.uk/publications/circular-200701-acceptable-use-internet-schools* *DE Circular 2011/22 Internet Safety:* *https://www.education-ni.gov.uk/sites/default/files/publications/education/2011%2022%20-%20Amended.pdf* *DE Circular 2016/26 Effective Educational Uses of Mobile Digital Devices accessible at:* *https://www.education-ni.gov.uk/publications/circular-201626-effective-educational-uses-mobile-digital-devices*

Topic/Issue	No.	Question	Response
			DE Circular 2013/25 - eSafety guidance: https://www.education-ni.gov.uk/publications/circular-201325-esafety-guidance *Schools are also reminded of C2k's advice regarding internet access - see document EN039: Managing Internet Filtering: https://www.c2kexchange.net/documentcentre/Documents/EN039%20-%20Managing%20Internet%20Filtering.pdf* *Information to be placed on Facebook should be treated as being made public. Careful consideration should be given as to what information is posted on Facebook, and official pages should be monitored closely. Schools should also provide pupils with information about the responsible use of social media.*
	22.2	Should all school Facebook pages be closed groups?	*This will depend upon what information the school is posting on the Facebook group or similar social media, or allowing to be posted there.* *A school sharing personal information with Facebook or any third party supplier requires a GDPR compliant data sharing agreement to be signed between the school and the supplier.* *EA will be supplying standard templates.*
	22.3	Is it ok to post pupil photographs on Facebook without adding pupil names?	*See 22.2*