CYNGOR SIR YNYS MÔN / ISLE OF ANGLESEY COUNTY COUNCIL	
Meeting:	Audit & Governance Committee
Date:	1 December 2020
Title of Report:	Anglesey Schools Data Protection Evaluation Report-First Evaluation Visit to Anglesey Primary and Secondary Schools by Schools Data Protection Officer- July 2020
Purpose of the Report:	To inform members as to the level of data protection compliance and risk in relation to schools
Report by:	Elin Williams, Schools Data Protection Officer Ext: 1833, dpoysgolionmon@ynysmon.gov.uk
Contact Officer:	Elin Williams, Schools Data Protection Officer Ext: 1833, dpoysgolionmon@ynysmon.gov.uk

Purpose of this report

To provide the Audit & Governance Committee with the Schools Data Protection Officer's analysis of where the schools are up to in terms of compliance with requirements under data protection legislation, mainly under the General Data Protection Regulation (*GDPR*) following first visit to primary and secondary schools.

This report gives a summary of findings of the Schools Data Protection Officer following the visits and offers next steps to take to ensure that all schools meet data protection requirements as soon as possible.

The report includes details around the findings of the visits to 45 schools between October 2019 and February 2020 and the steps taken following the visits up to July 2020.

Introduction

Following the appointment of a Schools Data Protection Officer in the Learning Service during August 2019, the officer undertook the first evaluation visit to 45 out of the 46 Anglesey primary and secondary schools.

The visits was also an opportunity to follow up on some of the action points that arose from the *Zurich Risk Engineering UK* inspection report (dated June 2019). The Council commissioned *Strategic Risk Practice Zurich Risk Engineering UK* to perform a review and to prepare an inspection report on data/information governance and the level of *GDPR* implementation across Anglesey schools.

The *Zurich* inspection identified 11 areas for action, with two of these being graded as 'High, eight as 'Medium' and one as 'Low'.

As a result of this report, an Action Plan was created between the Council's Audit and Risk Service and the Learning Service in order to respond to the points raised in

the *Zurich* report. Details regarding the developments around the actions points is included in the report.

The report also includes proposed steps to take that informs a work programme based on findings.

Summary of the Schools Data Protection Officer's Findings

- Day-to-day information management **practices** within schools are generally acceptable but the majority of schools with current key policies and documents have not been adopted and are in place as a number of these policies and documents were not created for schools prior to the appointment of the Schools Data Protection Officer. It is essential that current core policies and documents are adopted as soon as possible. COVID-19 has had an impact on the timetable for approving the key policies and documents but it is necessary to look to get these in place, in partnership with the schools, during the autumn term.

- There is a need to ensure that specific, effective and robust data protection processes are in place. This is in line with the key policies and documents. At present, there are no robust processes in place around handling breaches; handling data subject access requests; restricting access to personal information; the removal of personal data that has elapsed a retention period; managing data protection risks and creating Data Protection Impact Assessments for high risk processes.

- There is a need to ensure that schools have *ROPA* (including data flow maps) and an Information Asset Register in a place that are kept up-to-date.

- There is a need to ensure that schools have suitable and up-to-date Privacy Notices and that they are shared and are available to individuals and that data collection forms and consent forms include a summary of the Privacy Notice.

- There needs to be appropriate agreements in place with high level data processors and also with individual schools. The Schools Data Protection Officer will need to work with the schools to ensure that these are in place.

- The Schools Data Protection Officer needs to do more work with schools around the use of consent including reviewing the current forms.

- The training plan needs to be updated and schools ensure that all their staff have completed the online module.

- Work needs to be done to ensure that all school governing bodies are aware of their data protection responsibilities and how to ensure that schools comply. The school governing bodies will need to adopt the data protection

policies on behalf of the schools and ask schools to evidence their compliance with these.

Schools Data Protection Officer Assurance Assessment (July 2020)	Reasonable Assurance
The process of beginning to have policies, processes and practices in place to comply with data protection legislation has started within the schools, but there is more work to be done to have all schools on the same level and operating consistently across the island.	

Up-date on Progress since July 2020

It is noted that COVID-19 has had a significant impact on the implementation of the steps to be taken and on the work programme for approving the policies; adopting the policies and the training and awareness raising relating to this due to other key priorities arising during this period.

The following progress has been made since July 2020:

- The key policies, guidance and templates for schools have been finalised, translated and are ready to be shared and adopted by the schools.

- A Schools Data Protection Policy Plan is in place which details the dates of implementation of the different policies, guidance and key documents and templates and the training and support for the adoption of these that will be provided. Different key policies will be introduced and adopted from December 2020 up until July 2021 and a programme of dates have been arranged for the Schools Data Protection Officer to provide support and guidance to schools with the implementation of these.

- The School Data Protection Training Plan is in place. The training sessions arranged from November 2020 onwards are available online and through technology rather than just face-to-face sessions. This includes training for headteachers, teachers, schools staff and school governors.

- The Schools Data Protection Officer is undertaking a review of the use of consent and the current forms that are in use.

- Work is underway reviewing the use of systems, programmes and apps by the schools and to look at the agreements in place around these and the possible impact of Brexit on any agreements with providers based outside of the UK.

Recommendations

The Schools Data Protection Officer makes the following recommendations to the Committee, that:

i. the Schools Data Protection Officer report, including the findings, is accepted;

ii. the Committee endorses the Schools Data Protection Officer's proposed next steps to ensure that all schools operate in accordance with data protection requirements.

ANGLESEY SCHOOLS DATA PROTECTION EVALUATION REPORT

ELIN WILLIAMS, SCHOOLS DATA PROTECTION OFFICER

July 2020

Contents   Page

1. Background and Operational Summary

Following the appointment of a Schools Data Protection Officer in the Learning Service during August 2019, the officer undertook the first evaluation visits to Anglesey primary and secondary schools. These visits took place between October 2019 and February 2020.

The visits were undertaken as a starting point to see where schools are up to in terms of compliance with requirements under data protection legislation, mainly under the General Data Protection Regulation (*GDPR*) which came into force in May 2018. This also gave a better understanding to the Schools Data Protection Officer of what elements needed to be prioritised in terms of a work programme and was an opportunity to get to know key contacts within the school. It was also an opportunity to follow up on some of the action points that arose from the *Zurich Risk Engineering UK* inspection (see item 2 below).

Following the visits, the Schools Data Protection Officer came to the conclusion that day to day information management practices within the schools were acceptable but work needs to be done on ensuring that current key policies and documents have been adopted by the schools as soon as possible and it must be ensured that specific, effective and firm data protection processes are in place. It also needs to be ensured that risks are effectively managed and that appropriate agreements are in place with data processors. Having a specific training plan in place for staff and schools and the governing body is also a priority to ensure that everyone within the school structure is aware of their data protection responsibilities. It is essential that the schools understand their responsibilities and implications as the Data Controller and the legal expectations that come as a result. The Schools Data Protection Officer has identified what work must be done with the schools to ensure that they comply with data protection legislation and fulfil what is expected of them.

Schools Data Protection Officer Assurance Assessment (July 2020)	Reasonable Assurance
The process of beginning to have policies, processes and practices in place to comply with data protection legislation has started within the schools, but there is more work to be done to have all schools on the same level and operating consistently across the island.	

2. *Zurich Risk Engineering UK* Inspection

The Council commissioned *Strategic Risk Practice Zurich Risk Engineering UK* to perform a review and to prepare an inspection report on data/information governance and the level of *GDPR* implementation across Anglesey schools in 2019. The work included a situation questionnaire including specific *GDPR* scenarios for the education sector and also face to face interviews with 6 selected schools to understand their methods of handling and governing information and data protection. 25 of the 46 schools sent a response in terms of the questionnaire (55%) and 5 of the 6 schools were interviewed. *Zurich* also reviewed training materials that were part of the Council's *GDPR* programme.

One of the matters mostly highlighted in the report (dated June 2019) was that there was no Schools Data Protection Officer in place at the time. The company emphasised that the Data Protection Officer was a significant part missing in the review process as they were unable to discuss operational and strategic elements of data governance with the officer. The impact of not having a Schools Data Protection Officer in place for over a year in the *GDPR* implementation period was also seen during the visits by the Data Protection Officer.

The *Zurich Risk Engineering* UK inspection identified 11 areas for action, with two of these being graded as 'High, eight as 'Medium' and one as 'Low'.

As a result of this report, an Action Plan (APPENDIX A) has been created between the Council's Audit and Risk Service and the Learning Service in order to respond to the points raised in the *Zurich* report. When the Council's Audit and Risk Service reviewed the actions in October 2019, 'Reasonable' assurance was given for risk management, *GDPR* governance and management within the schools due to the appointment of a Schools Data Protection Officer (one of the 'High' risks) and the work done by her to address the points for action at the time.

The 11 actions that have arisen have been implemented or are in the process of being implemented and appear within this report. It is noted that COVID-19 has had an impact on the approval of the policies and this in its turn has had an impact on the original action timetable. (APPENDIX A) gives an update up to June 2020.

3. Visiting the Schools

An evaluation form (APPENDIX B) was used for visits and each school received a completed form with comments, including actions and main data protection risks identified by the Schools Data Protection Officer following the visit. A number of points within

the form coincide with the questions that pertain to *GDPR* within the '*School Management System*' so that schools are able to score themselves on where they have reached in terms of implementing *GDPR*.

The visit was in the form of a chat and this visit didn't go into detail in terms of seeing evidence of compliance. This will be something that will follow after schools receive more practical guidance and support on what specific policies and processes need to be in place. A visit took on average two hours to complete and something similar again to prepare the form to share with schools following the visit.

The Headteacher was present in the majority of visits and/or the person responsible for data protection at the school and other relevant officers were present. In the majority of primary schools, the Headteacher is responsible for data protection at the school. In the secondary schools, the Assisting Headteacher or another officer tends to be responsible for data protection matters.

These are the 45 schools who had a visit from the Schools Data Protection Officer between October 2019 and February 2020:

Primary Schools

Ysgol Gynradd Amlwch	Ysgol Esceifiog	Ysgol Llanfairpwll	Ysgol Penysarn
Ysgol Beaumaris	Ysgol Gymuned y Fali	Ysgol Llanfawr	Ysgol Rhoscolyn
Ysgol Gynradd Bodedern	Ysgol y Ffridd	Ysgol Llanfechell	Ysgol Rhosneigr
Ysgol Bodffordd	Ysgol Garreglefn	Ysgol Llangoed	Ysgol Rhosybol
Ysgol y Borth	Ysgol Goronwy Owen	Ysgol Llannerch-y-medd	Ysgol Rhyd y Llan
Ysgol Bryngwran	Ysgol y Graig	Ysgol Moelfre	Ysgol Santes Dwynwen
Ysgol Brynsiencyn	Ysgol Henblas	Ysgol Gymraeg Morswyn	Ysgol Santes Fair
Ysgol Cemaes	Ysgol Kingsland	Ysgol Parc y Bont	Ysgol Talwrn
Ysgol Corn Hir	Ysgol Llanbedrgoch	Ysgol Pencarnisiog	Ysgol y Tywyn
Ysgol Cybi	Ysgol Llandegfan	Ysgol Pentraeth	

Secondary Schools
Ysgol Uwchradd Bodedern
Ysgol Uwchradd Caergybi

Ysgol David Hughes
Ysgol Gyfun Llangefni
Ysgol Syr Thomas Jones

Special Schools
Canolfan Addysg y Bont

In contrast to the *Zurich* inspection, it is noted that all schools on the island apart from Ysgol Caergeiliog were part of the visits as they haven't yet confirmed whether or not they want to use the Schools Data Protection Officer service. The schools pay a contribution towards the post.

This report gives a summary of findings to the Schools Data Protection Officer following the visits and offers next steps to take to ensure that all schools meet data protection requirements as soon as possible. The report includes details around steps taken following the visits up to July 2020, including meeting with the Learning Service Senior Management Team on 20 July 2020 to discuss approving key data protection policies, guidelines and documents.

4. Registering with the Information Commissioner's Office *(ICO)*

Schools are required to pay an annual data protection fee to the *Information Commissioner's Office* as they process personal data. Almost all schools were registered with the Information Commissioner's Office during the visits.

Details of the Schools Data Protection Officer had been added against each school's registration.

It is important that schools ensure that they pay the fee on time, each year, to avoid the risk of being fined. This is being monitored by the Schools Data Protection Officer.

5. Records of Processing Activities *(ROPA)*

Under *GDPR*, schools need to have *Records of Processing Activities (ROPA)* in place. The schools did not have a *ROPA* in place during the visiting period. This had not been discussed in detail during the visits but this is an essential element to have in place.

The Schools Data Protection Officer has created a *ROPA* template and guide. It was agreed with the Senior Learning Service Management Team that work needed to be done with one of the primary schools and one of the secondary schools on the completion of *ROPA* which will be shared as a template for schools to use and adapt as necessary. Schools will need to keep this up-to-date and be responsible for updating it if there are any changes to data processing activities.

The Schools Data Protection Officer will also create data flow maps for different processes with the schools as part of this work.

6. Information Assets Register

Schools are required to have an up-to-date Information Assets Register which documents what personal data is held, where it came from, who it is shared with and what is done with the information.

The Information Assets Register template had been shared with schools by the Learning Service in summer 2018 so that they could use it to create a list themselves but some schools reported that this template was complex to use. As a result, the majority of schools did not have an Information Assets Register during the visits, with 10 (22%) of the schools with one in place or have tried to create one.

Work has already been undertaken with one of the primary schools on completing an Information Assets Register prior to the COVID-19 period, which will be used as a template for schools to use. The same will also need to be done with one of the secondary schools (this had originally been agreed for March 2020, but had to be postponed because of COVID-19).

The Senior Learning Service Management Team have confirmed that they are happy with the template. The Data Protection Officer will need to complete an Information Assets Register with a secondary school, and then share a primary and secondary template with the schools so that they can adapt it for their school. It is essential that everyone has a current one in a place that is regularly reviewed by the school.

7. Privacy Notice

12 (27%) of the schools had a Privacy Notice in place during the visiting period.

It is essential that schools have an up-to-date bilingual Privacy Notice which informs individuals about what personal information is collected and held by the schools. Individuals need to be informed of how the schools use their personal information and for what purpose. A Privacy Notice requires clarification of the purpose and legal basis for processing; identify any third party the school shares information with and any external processor also.

Some of the schools had created a Privacy Notice themselves. A template has been shared with schools by the Learning Service in summer 2018 for them to use to create their own Privacy Notice, but some schools reported that this template was complex to use.

The Schools Data Protection Officer has created a Privacy Notice template for primary and secondary schools and for the school workforce to create consistency. These are in the process of being approved by the Senior Learning Service Management Team and checked by relevant officers within the Council. The Schools Data Protection Officer is also in the process of creating a children and young people's version.

Schools will need to formally adopt the Privacy Notices; ensure that they are suitable for the school (modify them if not); be shared with individuals at the point of collecting information (e.g. the school's website or social media account) and updating and keeping them up-to-date as necessary.

The Schools Data Protection Officer will review all data collection and consent forms and include a summary of the Privacy Notice in these documents. Schools are responsible for ensuring that they are properly adopted and kept accurate and up-to-date.

8. Data Protection Policy

Some schools have an up-to-date Data Protection Policy in place. A Data Protection Policy was shared with schools by the Learning Service in 2018 for adoption following *GDPR* coming into force.

During the visits, 21 (47%) of the schools had adopted this policy and some still had the old pre-*GDPR* version in use which is not current policy. Some schools did not have a Data Protection Policy in place.
It is essential that all schools have a Data Protection Policy and that they monitor their compliance with the policy on a regular basis. Schools need to ensure that they can demonstrate that they comply with the policy and that they have a process in place to share this policy with individuals.

The Schools Data Protection Officer has updated the current School Data Protection Policy. The policy was originally due to be approved and adopted during the spring term but the schedule has slipped due to COVID-19. This is in the process of being approved by the Senior Learning Service Management Team and being checked by relevant officers within the Council. This is a key policy and it is important that schools adopt it as soon as possible and can demonstrate that they comply fully with this policy.

9. CCTV Policy

During the visiting period, 21 (72%) out of the 29 schools with a *CCTV* system had adopted the current *CCTV* Policy. It is essential that all schools with CCTV have a policy in place and also ensure that they have signs within *CCTV* monitored areas across the school that advertise that there is *CCTV* in operation. 16 of the schools did not have an active CCTV system during the visiting period.

The Schools Data Protection Officer has updated the current School *CCTV* Policy and created a School *CCTV* System Log for them to use. These are in the process of being approved by the Senior Learning Service Management Team and are being checked by relevant officers within the Council.

The schools with active *CCTV* will need to ensure that they have adopted the new policy and can demonstrate that they are fully compliant with this policy.

10. Information Risk Management

Schools did not have information risk management processes in place during the visiting period. Schools need a formal way of identifying risks around personal data e.g. Risk Register. This is a way for schools to be able to evidence that risks are identified and that mitigation is in place to deal with the risks. It is also important that the governing body is aware of any high information risks. This is in line with the Data Protection Impact Assessment process.

The Schools Data Protection Officer has created a Schools Data Protection Risk Register and a Schools Data Protection Risk Matrix. These are in the process of being approved by the Senior Learning Management Team and are being checked by relevant officers within the Council. Schools will be responsible for assessing and reviewing the risks and keeping the Risk Register accurate and up to date.

The Data Protection Officer will need to provide training around managing information risks to schools. This will be included in the Data Protection Training Plan.

11. Data Protection Impact Assessments *(DPIAs)*

Under *GDPR*, schools are legally asked to complete Data Protection Impact Assessments *(DPIAs)* when there is a high risk in data processing. Schools did not have a process in place around the completion of Data Protection Impact Assessments during the visiting period.

Schools are now aware of when they must carry out a Data Protection Impact Assessment (i.e. when they are using new technology that is likely to be high risk). They are also aware that the Schools Data Protection Officer needs to be involved in completing any Data Protection Impact Assessment.

The Schools Data Protection Officer has created a School Data Protection Impact Assessment Policy. This is in the process of being approved by the Senior Learning Service Management Team and being checked by relevant officers within the Council. The policy will be aligned with the School Data Protection Risk Register and the School Data Protection Risk Matrix. There is a Data Protection Impact Assessment template and a corporate Data Protection Impact Assessment Screening Checklist which will also be used for schools.

The Schools Data Protection Officer will undertake a piece of work around what current processes within the schools will require Data Protection Impact Assessments and training for relevant staff will need to be added to the Data Protection Training Plan so that schools are aware of their responsibilities.

12. Agreements with Processors

Schools did not appear to have individual agreements in place with data processors during the visiting period but this had not been discussed in detail. A high number of schools reported that they had no agreements as individual schools and used processors that all schools use.

Schools are aware that there is a need for a written contract with all third party providers who process personal data on behalf of the school. This can be a company that processes data through online educational programmes (e.g. through an app).

All schools have registered for the Wales Accord on the Sharing of Personal Information *(WASPI)* in the period May to July 2020. The *WASPI* Framework provides a practical working method to share personal information, provide common standards and templates for the development of Information Sharing Protocols *(ISPs)* and Data Disclosure Agreements *(DDAs).* The overall aim of the framework is to support public service providers to deliver effective services in complying with their legal obligations– i.e. *GDPR* and the *Data Protection Act 2018.*

The Schools Data Protection Officer will undertake a piece of work looking at high level agreements and also discuss with individual schools if agreements need to be in place with individual data processors. This work will be undertaken in autumn 2020.

13. Systems, Programmes and Apps Used by the Schools

The majority of schools had provided a list of all systems, programmes and apps used by schools that collect, share and process personal data during the visiting period.

This piece of work was originally being undertaken in order to prepare for the possibility of *a 'No Deal Brexit'* and to be able to prepare any agreements that needed to be changed. The Schools Data Protection Officer will use this information to review what agreements are in place with data processors during the autumn term 2020.

14. The Process of Investigating; Notifying of and Reporting Breaches

During the visits, schools shared that not many breach incidents had taken place in the past. As a result, most schools did not have an effective process to identify, report, manage, record and resolve any breaches of personal data in place. It is essential that all schools have a process in place for this.

Schools are aware that any breaches need to be reported to the Schools Data Protection Officer within 72 hours of being aware of a data breach in accordance with the requirements of the *ICO.* They are also aware that the Schools Data Protection Officer is responsible for deciding whether or not to report to the *ICO* and whether individuals need to be notified.

As there are no specific policies or templates for schools in place around dealing with breach proceedings, the Data Protection Officer has created a pack for dealing with these which includes:

- Schools Data Breach Policy;
- Schools Data Breach Guide;
- Schools Data Breach Investigation Form;
- Schools Data Breach Report to the School Governing Body; and
- Schools Data Breach Log.

The pack is in the process of being approved by the Senior Learning Service Management Team with relevant officers within the Council checking it. Schools will need to adopt the policy and ensure that there is a robust process in place in order to be able to deal with any cases within the statutory timescale. The Schools Data Protection Officer will need to provide training for relevant staff to ensure that there is a good understanding of the process within the schools and that they can evidence that they are complying with their responsibilities.

15. The Process of Handling a Data Subject Access Request

During the visits, schools shared that they tended not to receive many data subject access requests. Secondary schools received more requests than primary schools.

Under data protection legislation, individuals have the right to apply to access their personal information. It is important that schools have an effective process that deals with any data subject access request being received and can easily search for all records held about the individual. Requests need to be responded to within one calendar month even if the application comes in on a first day of the summer holidays. It is possible to have an additional two month extension in 'complex' cases.

As there were no specific policies or templates for schools in place around dealing with data subject applications, the Schools Data Protection Officer has created a pack for dealing with these which includes:

- Schools Data Subject Access Request Policy;
- Schools Data Subject Access Request Form;
- Schools Data Subject Access Request Acknowledgment Letter Template;
- Schools Data Subject Access Request Extension Letter Template; and

- Schools Data Subject Access Request Response Letter Template.

It is vitally important that the school has a good understanding of what data is being shared and what data is not appropriate to share (e.g. another person's personal data; third party data and excluded information). The Schools Data Protection Officer is available to facilitate and support schools in preparing information to share with individuals within the statutory timescale.

The pack is in the process of being approved by the Senior Learning Service Management Team with relevant officers within the Council checking it. Schools will need to adopt the policy and ensure that there is a robust process in place to be able to deal with any applications within the statutory timescale. The Schools Data Protection Officer will need to provide training for relevant staff to ensure that there is a good understanding of the process within the schools.

16. Keeping Personal Data Accurate and Up to Date

A majority of schools had processes in place to keep personal data accurate and up-to-date during the visiting period. It is essential that schools keep personal data accurate and up-to-date at all times and update information immediately when it is received. This reduces the risk of breaches. Individuals also have the right to ask to correct information that is inaccurate and this needs to be done in a timely manner.

The only element that can cause a delay in updating data is that some of the schools rely on the SIMS Officer to update the information as they do not have the rights to do this within the school. This can slow down the process as the SIMS Officers administer on behalf of a number of schools and are not located in the schools, so a delay can take place because of the circumstances.

Sometimes there are cases where the same information is held in many different places, so updating information can be difficult if the information is held by more than one person in more than one place. Schools need to ensure that they do not duplicate information unnecessarily and that information is updated on all versions of the information.

All schools need to ensure that there is an effective process in place that ensures that personal data remains accurate and up-to-date at all times to ensure that they comply with legal requirements. This is included in the general data protection training sessions.

17. Rights under GDPR

During the visits, schools were generally not fully aware of the different rights that individuals have under *GDPR.* This was not discussed in detail during the visits but this is included in the general data protection training, but more specific work needs to be done with relevant staff in order to improve their understanding of individuals' rights around their personal data, namely:

- The Right to Rectification and to Data Quality (Article 16);
- The Right to Erasure (Article 17);
- The Right to Restrict Processing (Article 18);
- The Right to Data Portability (Article 20);
- The Right to Object (Article 21);
- Rights in Relation to Automated Decision-Making and Profiling (Article 22).

There is more detail about these rights within the data protection policies.

18. Records Management Policy

Schools did not have a Records Management Policy in place during the visiting period and this was not discussed in detail. In order to ensure that effective records management is in place and to ensure that schools comply with data protection legislation, schools need a Records Management Policy.

A School Records Management Policy has been created by the Schools Data Protection Officer. The policy is in the process of being approved by the Senior Learning Service Management Team with relevant officers within the Council checking it. Schools will need to formally adopt the policy and ensure that they comply with this.

19. Consent- Consent and Data Collection Forms

A majority of schools used the current parental consent form to give their permission for the school to use pictures and images of their children for publication on a website, social media and newspapers. The majority of primary schools had systems to record and manage ongoing consent, but this can be challenging for secondary schools because of the numbers of pupils and the ability to manage and act on those that do not consent on different elements.

The Schools Data Protection Officer is reviewing the current consent forms to ensure that there is consistency across schools and that the use of newer technology is also included. The consent element can be complex and there is a general misunderstanding of the scope of appropriate use of this. The Schools Data Protection Officer needs to do more work with the schools around consent and create a Photo-taking Policy for the purpose of school publicity.

20. Secure Sharing of Information

A majority of schools used a school's official e-mail account for emailing during the visiting period. The schools have Welsh Government Hwb accounts and some also have County Council accounts. A majority of governors used personal e-mail addresses and some schools had *g-mail* accounts. The use of personal e-mail accounts for sharing personal data can be a risk.

It was discussed to put safeguards in place such as using only the initials of a name within e-mails when sharing personal details about pupils and using a password when documents containing personal data are shared by e-mail. There is a risk of data breaches occurring due to emails being sent to the wrong address etc. Safety measures are included in the general training sessions.

Schools need to ensure that all staff only use the school's official e-mail account and put safeguards in place around sending e-mails so that the risk regarding breaches taking place reduces and personal data is safer. Work is being undertaken to create Hwb accounts for all school staff and also for governors. This is a positive step towards ensuring that only official accounts are used for sharing personal data throughout the school.

The Schools Data Protection Officer has created a School Staff E-mail Policy and a School Information Security Policy and these policies are in the process of being approved by the Senior Learning Service Management Team and being checked by relevant officers within the Council. Schools will need to adopt the policies and ensure that they use the school's official e-mail account and put security measures in place when sending e-mails.

21. Records Retention Schedule

The current School Retention Schedule 2018 document was shared with schools in summer 2018. The document is based on national directions. This is the current document to use, but not all schools were aware of this during the visiting period.

The Senior Learning Service Management Team has confirmed to continue to use this version and to wait until regional work is undertaken to update it. It is important that retention periods are adhered to as the retention of personal data for longer than necessary goes against the principles of data protection legislation. Similarly, it is important not to dispose of personal data before the retention period ends either as there is a possibility that the information will be required for data subject access requests or for freedom of information requests.

The School Retention Schedule has been shared with the schools for use.

22. Processes and Arrangements for the Deletion and Disposal of Personal Data

The majority of schools had effective personal data deletion and disposal processes and arrangements in place during the visiting periods.

Most schools have suitable methods for disposing of paper documents (e.g. confidential waste bin, shredder). Some schools need to consider having a cross-cutting shredder that is safer than a standard shredder and consider paying a company that disposes of personal data securely when they have a large clearance operation.

The Schools Data Protection Officer has created a Schools Information Security Policy which includes arrangements for the safe removal and disposal of personal data. The policy is in the process of being approved by the Senior Learning Service Management Team with relevant officers within the Council checking it. Schools will need to formally adopt the policy and ensure that they comply with this and adhere to the School Retention Schedule.

23. Storage of Personal Data

Schools were able to list where personal data is stored (including paper and electronic records) and what security processes were in place during the visiting period.

Some of the schools raised that there were problems around storing personal information particularly in the schools in old buildings. There is not enough space in some buildings to store information securely. In addition, some schools are going to find it difficult to spend on buying lockable cupboards or furniture in order to protect personal data that is kept on open shelves within offices where the public have access to them as is currently the case in some schools.

Clearance of documents that have passed their retention date needs to take place in a number of the schools. There is a risk that personal information is still held in some schools when the legal time period has elapsed which breaches data protection rules.

There is work to do with some of the schools to make sure that they have a process in place of only giving access to personal data to appropriate officers who need to access the information only. Currently, not all schools have a system where access to information is restricted to only appropriate officers, which can be a risk. This is more evident with paper records than electronic records– this is due to a lack of space to store information effectively within buildings.

The Schools Data Protection Officer has created a School Records Management Policy, and the School Information Security Policy also deals with this. The policies are in the process of being approved by the Senior Learning Service Management Team and being checked by relevant officers within the Council. Schools will need to formally adopt the policies and ensure that they comply with them and have appropriate processes in place.

24. Data Protection Training

In discussing training with schools during the visits, most secondary and primary school Headteachers have received initial *GDPR* training in May 2018. Some secondary school staff have also received training from law firm *Geldards* in July 2019. It is noted that some Headteachers had not received any data protection training up to the visiting period.

All school staff were supposed to have completed the mandatory *GDPR* online module on the E-Learning Portal during June / July 2018. It appeared from the HR list that a large number of school staff had not completed this module and therefore the Schools Data Protection Officer asks that all those who have not completed it do so as soon as possible, as this is training that everyone in the Council has to do.

Data protection training needs were also identified during the visits. It was evident that most staff had not received formal training further to the online module and that staff needed to have a better understanding of *GDPR* and data protection in general.

Following on from this, the Schools Data Protection Officer has offered to provide a training session that focuses on practical issues and good practice that will be of use to employees in their day-to-day work and provides them with guidance on what their responsibilities are under *GDPR.* Most schools had shown an interest in holding a session with some having asked to do an

individual session for the school and others wanting to do it as a catchment area. Between January 2020 and February 2020, 14 schools received a general training session. 4 of these were sessions for individual schools and the remainder were part of the 2 catchment sessions arranged. Other sessions had been arranged between January 2020 and June 2020 but these were cancelled due to illness, weather or COVID-19.

GDPR training sessions for governors had been included within the overall training timetable for governors for the school year. Governors have a responsibility to ensure that the school complies with *GDPR* and it is a good idea to have a *GDPR* Champion on the governing board. This means that governors need an understanding of *GDPR* and their responsibilities and what is expected of them in their role. Only one training session with governors was held during the school year (in November 2019) instead of four due to illness and COVID-19, with only two governors having received the training to date.

The School Data Protection Training Plan is in place. The plan has been affected by COVID-19, so it is to be updated to include general sessions with school staff that were supposed to take place as well as governor training sessions. The new plan will also include sessions around specific data protection themes for relevant staff (e.g. information risk management, managing records, handling breach cases, handling data subject access requests and managing risks). The plan will be based on sessions for a 12 month period. The training sessions will need to be available online and through technology rather than just face-to-face sessions.

25. Conclusions

- Day-to-day information management **practices** within schools are generally acceptable but the majority of schools with current key policies and documents have not been adopted and are in place as a number of these policies and documents were not created for schools prior to the appointment of the Schools Data Protection Officer. It is essential that current core policies and documents are adopted as soon as possible. COVID-19 has had an impact on the timetable for approving the key policies and documents but it is necessary to look to get these in place, in partnership with the schools, during the autumn term.
- There is a need to ensure that specific, effective and robust data protection processes are in place. This is in line with the key policies and documents. At present, there are no robust processes in place around handling breaches; handling data subject access requests; restricting access to personal information; the removal of personal data that has elapsed a retention period; managing data protection risks and creating Data Protection Impact Assessments for high risk processes.

- There is a need to ensure that schools have *ROPA* (including data flow maps) and an Information Asset Register in a place that are kept up to date.
- There is a need to ensure that schools have suitable and up-to-date Privacy Notices and that they are shared and are available to individuals and that data collection forms and consent forms include a summary of the Privacy Notice.
- There needs to be appropriate agreements in place with high level data processors and also with individual schools. The Schools Data Protection Officer will need to work with the schools to ensure that these are in place.
- The Schools Data Protection Officer needs to do more work with schools around the use of consent including reviewing the current forms.
- The training plan needs to be updated and schools ensure that all their staff have completed the online module.
- Work needs to be done to ensure that all school governing bodies are aware of their data protection responsibilities and how to ensure that schools comply. The school governing bodies will need to adopt the data protection policies on behalf of the schools and ask schools to demonstrate their compliance with these.

The process of starting to have policies, processes and exercises in place to comply with data protection legislation has begun within the schools, but there is more work to be done to get all schools at the same level and operating consistently across the island.

26. Next Steps

The Schools Data Protection Officer has identified what pieces of work need to be done with the schools to ensure that they comply fully with data protection legislation and achieve what is expected of them as the Data Controller, who is ultimately responsible for ensuring that they process personal data legally. It is essential that schools understand their responsibilities and implications as the Data Controller and the legal expectations that come as a result. The Data Protection Officer is available to assist and facilitate this process and is available to provide advice and support to schools.

These are being proposed as next steps to ensure that all schools operate in accordance with requirements:

- For the policies, guidance, key documents and final templates to be formally approved by the Senior Learning Service Management Team, in partnership with schools, so that schools can formally adopt them in autumn 2020. All policies and documents will be available on the *GDPR* section of Addysg Môn so that everything in terms of current data protection

documents is available to schools in one place. The Schools Data Protection Officer has created the 'Anglesey Schools Data Protection Policy, Guidance and Key Documents Review Framework' document (ANNEX C) which provides an update on the status of the different documents that need to be adopted by schools (up to July 2020). **For schools to ensure that these policies have been formally adopted by the governing body and that they can demonstrate their compliance with the policies.**

- For the Schools Data Protection Officer to undertake work with schools to get *ROPA* (including data flow maps) and an Information Assets Register in place. To complete an Information Assets Register with a secondary school, and then share a primary and secondary template with the schools so that they can adapt it for their individual school.

- For the Schools Data Protection Officer to work with schools on adopting policies and creating processes for effectively handling data breaches and data subject access requests. To provide training with relevant staff so that schools can effectively handle breaches.

- For the Schools Data Protection Officer to complete the work of creating Privacy Notices and sharing them with the schools to adapt and adopt them. Also, to ensure that data collection forms and consent forms contain a summary of the Privacy Notice.

- For the Schools Data Protection Officer to work with schools to ensure that appropriate agreements are in place with high level data processors and also with individual schools. To start this work during the autumn term.

- For the Schools Data Protection Officer to undertake a piece of work and training sessions with schools around risk management and on how to complete Data Protection Impact Assessments. To review if Data Protection Impact Assessments have historically been undertaken for processing data that can be high risk and to work with schools to create any Data Protection Impact Assessments required. To start this work during the autumn term.

- For the Schools Data Protection Officer to review the current consent forms and to do more work with schools around consent and create a photo-taking policy for the purpose of school publicity.

- For the Schools Data Protection Officer to work with schools to ensure that they have processes around who has access to specific personal information and that information is kept securely within the schools. Also, to do work with some schools in terms of disposing of old documents that have passed their retention period.

- For the Schools Data Protection Officer to reorganise governors' data protection training sessions and complete the creation of the School Governing Body's Data Protection Guide. For governing bodies to ensure that members complete the training and are aware of their data protection responsibilities.

- For the Schools Data Protection Officer to update the general data protection training programme for school staff and governors. Also, to include more specific data protection training for relevant staff for the next 12 months e.g. to provide specific training around themes such as information risk management, records management and risk management. To look at providing training through technology such *as Microsoft Teams* or *Zoom* as well as sessions within the schools. For schools to ensure that relevant staff complete the training so that they understand their data protection responsibilities.
- For the Schools Data Protection Officer to prepare an annual data protection report from now on. The Senior Learning Service Management Team needs to confirm what will be included in the annual report but this is likely to be based on the number of breaches, the number of data subject requests, the number of data protection complaints, information around policies, a plan for next year, details of training and recommendations. It will also be based on pieces of work that the Schools Data Protection Officer will do in terms of monitoring schools' compliance with legislation, which will depend on looking for evidence of compliance by the schools.

APPENDIX A

SCHOOLS INFORMATION GOVERNANCE HEALTH CHECK FOLLOW UP

ACTION PLAN

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
1	A Schools DPO should be appointed at the earliest available opportunity – this role will provide the vital education support and guidance to the schools to address any current gaps in compliance to the new regulations Target date: 01/09/19	**H**	N/A	A Schools DPO commenced in post on the 19th August 2019.		Implemented August 2019.
2	If consent is deemed to be required there are a variety of self-sourced or adopted forms currently in use. Consider a single form, centrally owned with version control and electronically available. The DPO should also look to clarify when / why consent is required and in what circumstances.	**H**	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO is visiting each individual school to gain a better understanding of what forms are currently in use. Following the review, she will create a uniform library of forms and make them available centrally by 17.07.20. Second Follow Up (April 2020) Still work in progress and on track to be completed by 17.07.20.	**C3**	June 2020 School visits completed. SDPO visited every primary and secondary school during October 2019 to February 2020. Better understanding gained of what forms are currently in use. A uniform library of forms has been created. Forms will be approved by the Learning Senior Management Team on 20.07.20.

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
						Forms will not be available centrally by 17.07.20, but will be ready for September 2020. Approval of forms has been delayed due to COVID-19.
3	Consider extending Data Governance / GDPR training to School Governors.	L	N/A	First Follow Up (October 2019) Work in progress. The governors' training programme includes specific training arranged for governors: 'Governing Body responsibilities to ensure compliance with GDPR'. The Learning Service has scheduled training sessions for governors to complete by the end of the current school year (July 2020). Second Follow Up (April 2020) This is now delayed due to the Coronavirus. Session arranged for March was cancelled. Another session is due to take place in June, but will see if this can go ahead nearer the time.	C4	June 2020 The governors' training programme has been delayed due to COVID-19. Sessions arranged for March and June 2020 were cancelled as training sessions could not go ahead. To look at other ways of delivering the training e.g. via Zoom for the new school year (by January 2021).
4	Training – mix of approaches adopted across all schools visited. Combined with the responses there would appear to be a training refresh need. This could be done using existing training material with the situational case studies to support	M	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO is assessing training needs for all school staff during visits to each individual school.	C3	June 2020 Training Plan in place since 24.01.20. Several training sessions have been held, but some have been cancelled due to

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
	more granular understanding especially around social media and CCTV policies.			A training plan will be in place by 24 January 2020 that will schedule training sessions for the current school year. Second Follow Up (April 2020) Training Plan in place since 24.01.20. Several training sessions have been held, but some have been cancelled due to SDPO illness and Coronavirus. These will need to be rescheduled. It may be impossible to complete all remaining training sessions before 17.07.20 depending on the Coronavirus situation.		SDPO illness and Coronavirus. Training sessions will need to be rescheduled. It is impossible to complete all remaining training sessions before 17.07.20 due to COVID-19. To look at other ways of delivering the training e.g. via Zoom/Microsoft Teams for the new school year for those training sessions that have not been held (by January 2021).
5	The survey results ranged from annually to 3 years suggest (once appointed) the Schools DPO sets a standard policy review timetable / framework for review of data protection / data governance policies for increased clarity.	**M**	N/A	First Follow Up (October 2019) Work in progress. Following gaining a better understanding of current data protection / data governance policies during the visits to each school, the Schools DPO will review all policies during Spring term 2020. The Schools DPO will establish a Standard Data Protection Policy Review Framework by 31 January 2020. Second Follow Up (April 2020)	**C4**	June 2020 School visits completed and a better understanding gained of what current data protection/data governance policies are in place. SDPO undertook a review of all policies following the visits and has created a

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
				Standard Data Protection Policy Review Framework in place since 31.01.20. Schools Data Protection Policy in the process of being approved. Other policies in the process of being created.		Standard Data Protection Policy Review Framework which has been in place since 31.01.20. Dates of policy reviews have had to be pushed back due to COVID-19.
6	Scenario 1 1. Reviewing consent form to ensure request for consent is lawful and needed. 2. Retaining consent forms in line with retention periods as these forms would provide vital evidence in the event of an accident or other such incident.	**M**	N/A	First Follow Up (October 2019) Work in progress (as in 2 above). The Schools DPO will review consent forms during January 2020. She will create a uniform library of forms and make available centrally by 17.07.20. Second Follow Up (April 2020) Consent forms have been reviewed. Work is still in progress creating a uniform library of forms- still on track to be completed by 17.07.20.	**C3**	June 2020 Consent forms have been reviewed. A uniform library of forms has been created. Forms will be approved by the Learning Senior Management Team on 20.07.20. Forms will not be available centrally by 17.07.20, but will be ready for September 2020. Approval of forms has been delayed due to COVID-19.
7	Scenario 2 1. Reviewing CCTV usage policy and issuing standard	**M**	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO will review findings in February 2020 following her visits to	**C3**	June 2020 Findings of CCTV use has been gathered and included in the

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
	wording as to who can access / view images. 2. Ensuring a standard CCTV policy is in place for all schools (with CCTV in operation). 3. CCTV signs to be visibly displayed in all schools with CCTV systems.			the schools, and will create a standard CCTV Policy by 17/07/20. Second Follow Up (April 2020) Findings of CCTV use has been gathered and included in the reports following school visits (completed in February 2020). Work is still in progress in creating a standard CCTV Policy- still on track to be completed by 17.07.20.		reports following school visits (completed in February 2020). A standard CCTV Policy has been created and will be approved by the Learning Senior Management Team on 20.07.20. The policy will not be available by 17.07.20, but will be ready for September 2020. Approval of policies has been delayed due to COVID-19.
8	Scenario 3 1. Further training to be conducted or provided on social media / parents & pupils responsibilities and potential consequences – legal / reputational. 2. All schools to have a mandatory social media policy in place. Closed Facebook groups are in use and exist as a form of updating parents.	**M**	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO will create a standard Social Media Policy and arrange training around social media by 17.07.20. Second Follow Up (April 2020) Still work in progress and on track to be completed by 17.07.20.	**C3**	June 2020 A standard Social Media Policy has been created and will be approved by the Learning Senior Management Team on 20.07.20. The policy will not be available by 17.07.20, but will be ready for September 2020. Approval of policies

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
	3. All policies to have a review frequency in place – ranged from annually to 3 years.					has been delayed due to COVID-19. Will look at other ways of delivering the training around social media e.g. via Zoom/Microsoft Teams for the new school year (by January 2021).
9	Scenario 4 1. For schools with CCTV in operation DPIA to be conducted. 2. All schools to display CCTV signs / usage. 3. CCTV policies to be updated and reflective of responsibilities and appropriate usage. 4. Where there is no CCTV consider widening installations to encompass all schools estates for consistency in usage, application and policy – linked to safeguarding.	**M**	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO will support schools to complete Data Protection Impact Assessment (DPIA) and create a standard CCTV Policy by 17/07/20. Second Follow Up (April 2020) Still work in progress and on track to be completed by 17.07.20.	**C3**	June 2020 A standard CCTV Policy has been created and will be approved by the Learning Senior Management Team on 20.07.20. A Data Protection Impact Assessment (DPIA) Policy has been created and will be approved by the Learning Senior Management Team on 20.07.20. SDPO will need to arrange to support schools to complete DPIA during the new school year. This will

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
						not be completed by 17.07.20. The policies will not be available by 17.07.20, but will be ready for September 2020. Approval of policies has been delayed due to COVID-19.
10	Scenario 5 1. Advice given to schools on what can / cannot be viewed including advice on redaction of information. 2. All schools to adopt a uniform response timeframe in line with GDPR timeframes / guidance. 3. Check if Standard Access Request form exists – potential for e-form. 4. Ensure schools are aware that incorrect information can be corrected if proved to be inaccurate.	**M**	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO will create guidance and a standard form around Data Subject Access Requests for schools to use following visiting schools. She will also create guidance around correcting inaccurate information by 21.02.20. Second Follow Up (April 2020) Delayed. Work in progress- policy, guidance and standard form in the process of being created. Will be ready mid-April 2020.	**C3**	June 2020 Data Subject Access Request Policy, guidance and standard form created and correcting accurate information guidance created and will be approved by the Learning Senior Management Team on 20.07.20. Policies, guidance and documents were not available for 21.02.20, but will be ready for September 2020.
11	Scenario 6 1. All schools to review email policy and include a case study or the correct answer to this scenario as standard all	**M**	N/A	First Follow Up (October 2019) Work in progress. The Schools DPO will create a standard E-mail Policy and guidance around data breaches by 21/02/20.	**C3**	June 2020 A standard E-mail Policy and guidance around Data Breaches have been created and

Ref	Risk / Issue	Risk Rating	Management Response	Follow Up Results	Revised Risk Rating	Status / Revised Completion Date
	staff should be made aware of the escalation routes and breach recording timeframes. 2. Ensure schools record corrective actions and evidence this should this event occur.			<u>Second Follow Up (April 2020)</u> Delayed. Work in progress- E-mail Policy and guidance around data breaches are in the process of being created. Will be ready mid-April 2020.		will be approved by the Learning Senior Management Team on 20.07.20. Policy and guidance were not available by 21.02.20, but will be ready for September 2020.

APPENDIX B

School Data Protection Processes and Practices Evaluation Form

First Visit by the Schools Data Protection Officer

Details of Visit	
School	
Date	
Person met with and their role	
Name and details of individual responsible for data protection at the school	

1. Information Commissioner's Office (ICO) Registration		
1.1.	The school is registered with the Information Commissioner's Office- yes/no	
1.2.	The school's registration number	
1.3.	Registration renewal date	
1.4.	Details of the Schools Data Protection Officer are on the registration- yes/no	

1.5.	Any actions to be taken	

2. Schools Data Protection Officer		
2.1.	The contact details of the Schools Data Protection Officer are on the school website- yes/no	
2.2.	Are the appropriate staff at the school aware that there is a Data Protection Officer in place- yes/no	
2.3.	Any actions to be taken	

3. Records of Processing Activities (ROPA)- Article 30 of GDPR		
3.1.	The school is aware that a Records of Processing Activities is needed and has one in place- yes/no	
3.2.	Any actions to be taken	

4. Information Asset Register		
4.1.	The school has completed an Information Asset Register documenting what personal data is	

	kept, from where it came, with whom it is shared and what is done with it- yes/no	
4.2.	The school has data flow maps- yes/no	
4.3.	Any actions to be taken	

5. Privacy Notice – Article 14 GDPR		
5.1.	The school has an up-to-date Privacy Notice explaining the purpose and legal basis for processing; that notes any third party that the school shares information with and any external processor- yes/no	
5.2.	The school has a Privacy Notice specifically for children if the school offers online services directly for children- yes/no	
5.3.	The Privacy Notice is on the school website- yes/no	
5.4.	There is a process in place to share the Privacy Notice if a verbal request is made- yes/no	
5.5.	The school has added a summary of the Privacy Notice to the data collection forms which are sent to parents/pupils- yes/no	
5.6.	Any actions to be taken	

6. Data Protection Policy - Article 24(1) of GDPR	
6.1.	The school has adopted and is following a suitable Data Protection Policy- yes/no	
6.2.	The school monitors its compliance with the Data Protection Policy- yes/no	
6.3.	The Data Protection Policy is available on the school website- yes/no	
6.4.	There is a process in place to share the Data Protection Policy if a verbal request is made- yes/no	
6.5.	Does the school have any other policies pertaining to data protection- yes/no	
6.6.	Any actions to be taken	

7. CCTV Policy - Article 29 of the Protection of Freedom Act 2012	
7.1.	The school has a CCTV Policy in place- yes/no	
7.2.	The CCTV Policy is on the school website- yes/no	

7.3.	There is a process in place to share the CCTV Policy if a verbal request is made- yes/no	
7.4.	The school has signs within all areas across the school that are monitored by CCTV that notify that there is CCTV in operation- yes/no	
7.5.	Any actions to be taken	

8. Information Risk Management		
8.1.	The school has a process in place that manages information risks- yes/no	
8.2.	Any actions to be taken	

9. Data Protection Impact Assessment- Article 35 of GDPR		
9.1.	The school is aware of when it must conduct a Data Protection Impact Assessment (new technology- systems/programmes/apps by any third party)- yes/no	
9.2.	The school is aware that the Schools Data Protection Officer can assist in completing a Data Protection Impact Assessment- yes/no	

9.3.	Any actions to be taken	

10. Data Processing Agreements- Article 28(3) of GDPR		
10.1.	The school is aware that a written contract is required and that a written contract is in place with each third party provider that processes personal data on behalf of the school- yes/no	
10.2.	Any actions to be taken	

11. Systems, Programmes, Apps used by the School		
11.1.	The school has provided a list of all systems, programmes and apps used by the school that gather, share and process personal data- yes/no	
11.2.	Any actions to be taken	

12. Process of Investigating, Notifying and Recording Data Breaches - Statement 87; Article 33(1) and Article 33(5) of GDPR		
12.1.	The school has effective processes to denote, report, manage, record and	

	solve any personal data breaches- yes/no	
12.2.	The school is aware that any data breaches must be reported to the Schools Data Protection Officer- yes/no	
12.3.	The school has a log for data breach incidents and has incident report forms on file- yes/no	
12.4.	Any actions to be taken	

13.	**Process to Deal with Data Subject Access Requests - Article 15 of GDPR**	
13.1.	The school has an effective process that deals with any data subject access request received and can easily search for all records held on the individual- yes/no	
13.2.	The school is aware that the Information Commissioner's Office expects schools to respond to data subject access requests within a month even if the request is made during school holidays- yes/no	
13.3.	Any actions to be taken	

14.	Maintaining Accurate and Up-to-date Personal Data	
14.1.	The school has processes to ensure that the personal data it retains continues to be accurate and up-to-date- yes/no	
14.2.	Any actions to be taken	

15.	Rights in terms of GDPR	
15.1.	The school is aware of individuals' different rights under GDPR and is aware that some of these aren't appropriate in the context of schools since some tasks and information must be statutorily retained but requests may be made around: • Right to Rectification (Article 16) • Right to Erasure (Article 17) • Right to Restriction of Processing (Article 18) • Right to Data Portability (Article 20) • Right to Object (Article 21) • Right to Object to Automated Processing, Including Profiling (Article 22)	
15.2.	Any actions to be taken	

16.	Records Management Policy - Section 46 Code of Practice (FOI Act 2000)	
16.1.	The school has a Record Management Policy in place- yes/no	
16.2.	Any actions to be taken	

17.	Consent – Consent and Data Collection Forms- Data Protection Act 2018 and Article 4 and 7 of GDPR	
17.1.	The school has consent forms for the processing of personal data which gives parents and pupils the option to 'opt in' (e.g. photos, trips)- yes/no	
17.2.	The school has systems to record and manage continuous consent and a specific timetable to do so- yes/no	
17.3.	The school has a method of managing and acting upon those who do not provide consent for different elements- yes/no	
17.4.	Any actions to be taken	

18.	Sharing Information Safely	

18.1.	The school uses a secure email address to send electronic personal data- yes/no	
18.2.	Any actions to be taken	

19. Records Retention Schedule - Section 46 Code of Practice (FOI Act 2000)		
19.1.	The school is aware of and is complying with the Records Retention Schedule- yes/no	
19.2.	Any actions to be taken	

20. Processes and Arrangements for Deleting and Discarding Personal Data		
20.1.	The school has a process of securely discarding personal data that is no longer required- yes/no	
20.2.	The school is aware of the principle of not retaining personal data for longer than required but that some documents are to be retained for specific periods in line with the Record Retention Schedule- yes/no	
20.3.	The school has suitable methods of discarding paper documents (e.g.	

	confidential waste bin, shredder)- yes/no	
20.4.	Any actions to be taken	

21. Personal Data Storage - Section 46 Code of Practice (FOI Act 2000)		
21.1.	The school can list where personal data is stored (including paper and electronic records) and the safety processes that are in place- yes/no	
21.2.	The school has a process in place to lock paper records away and for only the appropriate officers to have access to them- yes/no	
21.3.	The school has a process in place to ensure that electronic records are stored in a safe place and that there is a process in place so that only the appropriate staff are able to access them- yes/no	
21.4.	The school has a process in place regarding using devices such as memory sticks- yes/no	
21.5.	The school is aware to not use e-mail accounts as means to store information and that emails must be deleted/filed appropriately- yes/no	
21.6.	The school is aware not to place personal data up on noticeboards	

	unless there is a legal basis to do so (e.g. notification of a food allergy or medical condition)- yes/no	
21.7.	The school has a process in place to ensure that staff don't take photos or record pupils on personal devices- yes/no	
21.8.	Any actions to be taken	

22. Data Protection Training – Article 5(2) of GDPR		
22.1.	Who at the school has completed data protection awareness training	
22.2.	Who at the school requires training/further training?	
22.3.	Does the school have a process in place of recording who has completed training- yes/no	
22.4.	Any actions to be taken	

23. Main Risks Identified

24. Any Additional Comments, Suggestions and Requests by the School

Headteacher's Signature	
Date	
Schools Data Protection Officer's Signature	
Date	

APPENDIX C

Anglesey Schools Data Protection Policy, Guidance and Key Documents Review Framework

No.	Policy, Guide, Key Document	Progress Update	Review Timetable
1	Schools Data Protection Policy (review current policy)	Policy discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the policy to be ready for adoption by the schools in **Autumn 2020.** Original adoption date pushed back due to COVID-19.	Annually- review **July 2021** for Autumn term 2021.
2	School Data Breach Pack: 1. Schools Data Breach Policy 2. Schools Data Breach Guidance 3. Schools Data Breach Investigation Form 4. Schools Data Breach Report to the School Governing Body 5. Schools Data Breach Log	Pack discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the pack to be ready for adoption by the schools in Autumn 2020. Original adoption date pushed back due to COVID-19.	Every 2 years- **review July 2022** for the Autumn term 2022.
3	Gwynedd and Anglesey Procedure for Sharing Information with United Kingdom Police Authorities	Procedure approved by the Senior Learning Team on 20.07.20. Procedure ready for adoption by schools **Autumn term 2020.** Original adoption date pushed back due to COVID-19.	Every 3 years- **review July 2023** for the Autumn term 2023.
4	School Retention Schedule (current version 2018)	The Senior Learning Team confirmed on 20.07.20 to stick to the current version and review it as part of regional work. This version was re-shared with all schools on 23.07.20.	As necessary (depending on national guidance)

5	School Privacy Notice: 1. Primary Schools 2. Secondary Schools 3. School Workforce 4. **Children and Young People's Version**	Pack discussed with the Senior Learning Team on 20.07.20. Need to create a children and young people's version for primary and secondary schools. Need to confirm elements with relevant Council officers. Aim for the pack to be ready for adoption by the schools in Autumn 2020. Original adoption date pushed back due to COVID-19.	As necessary (when there is any change)
6	Schools Information Security Pack: 1. Schools Information Security Policy 2. Schools Information Security Investigation Form	Pack discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the pack to be ready for adoption by the schools in Autumn 2020.	Every 2 years- **review July 2022** for the Autumn term 2022.
7	Schools Data Subject Access Request Pack: 1. Schools Data Subject Access Request Policy 2. Schools Data Subject Access Request Form 3. Schools Data Subject Access Request Acknowledgment Letter Template 4. Schools Data Subject Access Request Extension Letter Template 5. Schools Data Subject Access Request Response Letter Template	Pack discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the pack to be ready for adoption by the schools in Autumn 2020. Original adoption date pushed back due to COVID-19.	Every 3 years- **review July 2023** for Autumn term 2023.
8	School Staff E-mail Policy	Policy discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the policy to be ready for adoption by the schools in Autumn 2020. Original adoption date pushed back due to COVID-19.	Every 2 years- **review July 2022** for the Autumn term 2022.

9	Schools Data Protection Impact Assessment Pack: 1. Schools Data Protection Impact Assessment Policy 2. Schools Data Protection Risk Register 3. Schools Data Protection Risk Matrix 4. Data Protection Impact Assessment Template 5. Data Protection Impact Assessment Screening Checklist	Pack discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the pack to be ready for adoption by the schools in Autumn 2020.	Every 3 years- **review July 2023** for the Autumn term 2023.
10	Schools CCTV System Package: 1. School CCTV Policy (review of current policy) 2. School CCTV System Log	Pack discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the pack to be ready for adoption by the schools in Autumn 2020. Original adoption date pushed back due to COVID-19.	Every 3 years- **review July 2023** for the Autumn term 2023.
11	Schools Records Management Policy	Policy discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the policy to be ready for adoption by the schools in Autumn 2020.	Every 3 years- **review July 2023** for the Autumn term 2023.
12	School Staff Social Media Policy	Policy discussed with the Senior Learning Team on 20.07.20. Need to confirm elements with relevant Council officers. Aim for the policy to be ready for adoption by the schools in Autumn 2020. Original adoption date pushed back due to COVID-19.	Every 2 years- **review July 2022** for the Autumn term 2022.
13	Schools Records of Processing Activities Pack (ROPA):	Senior Learning Team confirmed on 20.07.20 to approve the package. Work needs to be done with one primary school and one secondary school on completing the template. To be used as a template to	Every 3 years- **review July 2023** for the Autumn term 2023.

	1. Schools Records of Processing Activities Guide (ROPA) 2. Schools Records of Processing Activities Template (ROPA)	be adapted as required by all schools during the **Autumn 2020 term.**	
14	Schools Information Assets Register Template	The Senior Learning Team confirmed on 20.07.20 to continue to use the current version as a template. Work has already been done with one primary school on completing the register. This also needs to be done with one secondary school. To be used as a template to be adapted as required by all schools during the **Autumn term 2020.**	Every 3 years- **review July 2023** for the Autumn term 2023.
15	Schools Data Protection Bilingual Glossary of Terms, Definitions and Legislation	Need to complete the document and share it with all schools during the **Autumn term 2020.**	As necessary (when there is any change).
16	Consent Form Pack: 1. Parental Consent Form 2. Biometric Systems Use Consent Form	Need to complete the pack and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it to be ready for adoption by the schools in Autumn 2020**.**	Every 3 years- **review July 2023** for the Autumn term 2023.
17	Photo-taking Policy for the purpose of School Publicity	Need to complete the policy and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it to be ready for adoption by the schools in Autumn 2020**.**	Every 3 years- **review July 2023** for the Autumn term 2023.
18	School Governing Body Data Protection Guide	Need to complete the guidance and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it to be ready for adoption by the schools in Autumn 2020**.**	Every 2 years- **review July 2022** for the Autumn term 2022.

19	Schools Personal Data Classification Policy	Need to complete the policy and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it to be ready for adoption by the schools **in Spring term 2021.**	Every 2 years- **review November 2022** for Spring 2023 term.
20	Schools Information Risk Policy	Need to complete the policy and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it to be ready for adoption by the schools in **Spring term 2021**.	Every 3 years- **review November 2023** for Spring term 2024.
21	Schools Personal Data Processing Policy	Need to complete the policy and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it in to be ready for adoption by the schools in **Spring term 2021**.	Every 3 years- **review November 2023** for Spring term 2024.
22	School Special Category Personal Data Processing Policy	Need to complete the policy and then share it with the Senior Learning Team, relevant Council officers and schools, in order to approve it to be ready for adoption by the schools **in Spring term 2021.**	Every 3 years- **review November 2023** for Spring term 2024.