CYNGOR SIR YNYS MÔN / ISLE OF ANGLESEY COUNTY COUNCIL	
Meeting:	Governance and Audit Committee
Date:	8 February 2024
Title of Report:	Report of the Schools Data Protection Officer on the Outcome of the Information Commissioner's Office's Investigation into the Cyber Incident in June 2021
Purpose of the Report:	To inform members as to the outcome of the investigation conducted by the ICO following reporting the cyber incident affecting the secondary schools.
Head of Service:	Marc Berw Hughes Director of Education, Skills and Young People MarcHughes@ynysmon.gov.wales
Report Author:	Elin Williams Schools Data Protection Officer dpoysgolionmon@ynysmon.gov.wales

Purpose of this report

To provide the Audit and Governance Committee with an overview of the outcome of the Information Commissioner's Office's (ICO) investigation into the cyber incident at the secondary schools in 2021.

The report also provides an overview of what actions have been taken by the Schools Data Protection Officer and the Council's ICT Service in terms of forming an internal work programme to address various technical and information governance elements that were deficient.

Recommendations

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

> i. the Schools Data Protection Officer's report, providing an overview of the outcome of the ICO's investigation into the incident, is accepted.
> ii. the actions identified and completed via the internal work programme are accepted.

Report by the Schools Data Protection Officer on the Outcome of the Information Commissioner's Office's Investigation into the Cyber Incident in June 2021

1. Background

It was discovered on the 23rd of June 2021 that a potential cyber-incident had occurred which affected all the five secondary schools on Anglesey - Ysgol Syr Thomas Jones; Ysgol Uwchradd Bodedern; Ysgol Gyfun Llangefni; Ysgol David Hughes and Ysgol Uwchradd Caergybi.

It was not known at the time if personal data held on the schools' systems could have been compromised during the incident. The alarm was raised following discovering suspicious traffic on secondary school e-mail servers.

Information technology systems, including e-mail accounts, had been temporarily disabled to contain the incident at the time. There was disruption at the schools whilst the incident was being contained.

A team of specialised cyber-technology consultants were immediately brought in by the Council to investigate the incident. The National Cyber Security Centre (NCSC) also provided support to resolve matters. Forensic analysis of the cyber incident found no evidence that ICT systems were infiltrated or compromised.

The incident was reported to the Information Commissioner's Office (ICO) due to the possible risk to the highly sensitive records held by the schools.

2. Actions Completed as Part of the Internal Work Programme Following Secondary Schools Cyber Incident

2.1. Overview

Following the incident in June 2021, an internal work programme was formed that contained several important and far-reaching remedial steps to address various technical and information governance elements that were deficient.

Technical and data protection governance improvements have been led by the Schools Data Protection Officer and the Council's ICT Service officers.

Several important actions have been completed since the programme was implemented, including accepting key data protection policies, and upgrading information technology systems and infrastructures in schools.

The incident prompted the Council to bring forward planned works, as part of the Welsh Government's HWB programme, to upgrade information technology systems of the secondary, special and primary schools. The work to upgrade the ICT systems and infrastructure began over the 2021 summer holidays.

Data systems that the schools were using were transferred on to the HWB cloud services. Being on HWB has helped make the systems at the schools as robust as possible and has reduced the risk of any potential cyber-attack or incidents in the future.

Work was undertaken to enable Multi Factor Authentication (MFA) on HWB accounts of staff and school governors to improve security when accessing HWB from home.

As part of the response to the incident, it was decided to move the equipment used by schools to Microsoft InTune, again to improve access security. The migration has been completed for the primary schools and Canolfan Addysg y Bont, with work being started on the migration of secondary schools.

2.2. Data Protection Governance Improvements

No	Actions and Improvements	Progress Since July 2021
1	To update current data protection policies and to create new policies.	A total of **14** data protection policies have been either updated following the adoption of the *UK GDPR* or created as new policies for schools: • Schools Data Protection Policy. • Schools Data Breach Policy. • Schools Information Security Policy. • Procedure for Sharing Information with Police Authorities in the United Kingdom (Gwynedd & Anglesey). • Schools Data Subject Access Request Policy. • Schools Data Processing Policy. • Transferring School Records to the Anglesey Archives Policy. • Schools Data Protection Impact Assessment Policy. • Schools CCTV Policy. • Schools Record Management Policy. • Schools E-Safety Policy. • School Staff Email Policy. • School Staff Social Media Policy. • Taking Photos for the Purpose of School Publicity Policy. A Data Protection Policies Checklist document has been developed to support schools to confirm that they have actioned the main requirements within all the data protection policies.

2	To ensure school staff and governors have received data protection training and are aware of their responsibilities in terms of data protection compliance.	Training sessions have been held with headteachers, school staff and governors. A total of **51** training sessions have been held between July 2021 and November 2023 and **25** governing bodies have been audience to a data protection presentation.
3	To use the School Management Review (SMR) to monitor compliance and to confirm which policies have been adopted by schools.	The School Management Review was used to gain baseline information regarding compliance and is used to monitor which schools have adopted which data protection policies.
4	To create a Service Level Agreement between schools and the Council for the Schools Data Protection Officer service.	A Service Level Agreement was created and shared with schools to sign in November 2021 following a period of consultation. The current SLA will be reviewed in March 2024.
5	To map the data flow between the schools and the Council.	A group was established to look at contracts and the processes in place between schools and the Council to identify where an agreement is required. Work is ongoing with this workstream.
6	To review arrangements with Data Processors and create/review Data Processing Agreements where required.	Mapping work around which systems, programmes, and apps that each individual school uses has been completed. This has provided information on whether schools already had appropriate data protection agreements in place and further work has been completed to create new Data Protection Agreements where needed and when new apps and programmes are used. Work is ongoing with this workstream.
7	To create a Record of Processing Activities (ROPA) Package and Information Asset Register Package.	A guidance document on how to create a ROPA was developed. Instead of providing a template for schools to complete themselves, the Schools Data Protection Officer has instead been developing a pre-populated ROPA template for schools to adapt (both a primary and secondary version). This also includes an Information Asset Register. These have been developed using the information gathered from the mapping exercise regarding which systems, programmes and apps are used. The templates are ready to be approved and sessions will be held to support schools with adapting the templates.
8	To create a Schools Data Protection Impact Assessment Package.	A risk register template and risk matrix were developed and shared with schools to support

		individual schools with identifying and monitoring data protection risks.
9	To complete Data Protection Impact Assessments.	A general DPIA template has been created for relevant schools to adapt for their CCTV system. Work is ongoing with this workstream.
10	To create a consent form package.	The current consent form for publishing photographs on various platforms has been reviewed and updated and a leaflet has been produced to explain to pupils and parents how *UK GDPR* consent works.
11	Conduct a data protection audit.	The Schools Data Protection Officer has visited each individual school to review data protection compliance and arrangements both in 2022 and 2023.
12	Discuss schools' data protection matters with the Primary and Secondary Forums and share the school data protection update newsletter.	The Schools Data Protection Officer provides regular updates to schools which includes sharing a termly newsletter. There is also a schools data protection section within the school governor bulletin and regular updates and information relating to data protection are provided via the Learning Service weekly bulletin. The Schools Data Protection Officer is regularly invited to attend the Primary Strategic Forum and Secondary Strategic Forum meetings and is also a member of the Schools ICT Forum and the Improving Processes and Systems Working Group. There is a data protection page on the Learning Service microsite where all current policies, guidance and templates are available for schools to use, and a Schools Data Protection Operational Group has been established.

2.3. ICT Improvements

The following are improvements suggested by the company that supported the Isle of Anglesey County Council following the secondary schools cyber incident (NCC Group).

No	Suggested Improvements	Progress to Date
1	**Upgrade from legacy operating systems**	By migrating to InTune, current versions of Windows installed or the computer has been de-commissioned if installing updates was not possible.
2	**Implement Multi Factor Authentication (MFA)**	MFA in place via InTune. Any requests to log in from outside of the school network requires MFA.

3	**Disable legacy email protocols (IMAP & POP3)**	This has been addressed by the use of the HWB email system.
4	**Up-to-date anti-virus scan**	All equipment that has been migrated to InTune receives Defender updates.
5	**Microsoft local administrator password solution**	Equipment has administrator accounts that are unique and complicated, details are securely stored by the ICT team.
6	**Remote desktop hardening**	Remote desktop has been disabled.
7	**Restrict internet access**	Access to the internet has been disabled from servers.
8	**Deploy Endpoint Detection and Response (EDR)**	Need to prepare a business case once the secondary schools' migration has been completed.
9	**SIEM solution**	SIEM has been installed corporately, work has begun to look at importing school data.
10	**Account privileges**	Accounts on equipment are not administrator accounts.
11	**Review patch management**	Updates are managed via InTune settings, and the infrastructure team are organising updates for other packages as needed.
12	**Review potentially unwanted programmes**	All computers reconfigured and only software that is approved is installed.

3. Information Commissioner's Office Outcome to their Investigation

The ICO shared its outcome to its investigation following the Council reporting the incident to them in June 2021, via a letter in April 2023. The ICO confirmed that the incident had been considered under the UK General Data Protection Regulation (UK GDPR) due to the nature of the processing involved and that no further intervention was required by them.

It was recognised by the ICO that during investigations into the incident, it was found that various technical and information governance elements that are needed to comply with the relevant legislation were deficient. The technical deficiencies were highlighted in a report by the NCSC (National Cyber Security Centre), the UK's main specialist in cyber security.

Additionally, the ICO offered encouragement to continue with the technical and data protection governance improvements in the schools.

4. Conclusions

It is clear that the Council's ability to recognise and identify what needed to be adopted and improved upon was acceptable to the ICO, and that this has prevented further intervention.

The Schools Data Protection Officer and the Council’s ICT Service officers have continued with the technical and data protection governance improvements in the schools, as recommended by the ICO.

Continuing with the work programme is crucially important in order to create a secure digital infrastructure and a strong culture of data protection at our schools. The Schools Data Protection Officer and the Council’s ICT Service will continue to support schools to complete the work programme and to ensure that every school has the policies, key documents, best practices, and the appropriate technology to be able to fully comply with data protection requirements.

Cyber-attacks still pose a real threat to schools, but the upgrading of the systems and infrastructure, along with good data protection compliance practices, puts schools in a safer situation going forward.