Internal Audit Report

Operations

SEEMiS

Issued to:
Rob Polkinghorne, Chief Operating Officer
Graeme Simpson, Chief Officer – Integrated Children's and Family Services
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
Eleanor Shepherd, Chief Education Officer
External Audit

Date of Issue: February 2020 **Report No. AC2021**

EXECUTIVE SUMMARY

SEEMiS provides the management information needs of all Aberdeen City Council schools as well as a wide range of central administrative and quality improvement functions. It is used for the maintenance of personal and academic (including SQA) records for pupils; personal information and work records for staff; and attendance records for pupils and staff.

The objective of this audit was to provide assurance that appropriate control is being exercised over the system in view of the perceived criticality of the system and the significant volume of sensitive personal data held.

Whilst access to and removal from the system for non-school staff is controlled via an online portal, at a school level this is managed by school system administrators and the majority of access is set up based on verbal requests by the school's senior management team. Education has agreed to introduce a documented approval process for providing system access at a school level. It was also noted that a number of former employee "work records" within the system remained current and that certain employees had access to records of schools where they no longer worked. The Service has agreed to address this by: disabling accounts where required; updating procedures in relation to removing access; and scheduling regular reviews of user access.

As at November 2019, 362 current system users had not completed the mandatory Information Governance training, which covers data protection requirements under the General Data Protection Regulation (GDPR). As SEEMiS holds personal information about both pupils and staff, the Service has agreed to instruct staff to complete the Information Governance training and will consider establishing a requirement to complete this training before access is granted to the system.

A Data Sharing Agreement is in place with the SQA, however the agreement is historic and predates the introduction of the data protection requirements under the GDPR. The Service has agreed to complete a Data Protection Impact Assessment for SEEMiS to identify all personal data sharing with third parties, the related risks and to ensure data sharing agreements in place cover routine sharing of personal data with third parties.

In accordance with data protection legislation, any arrangement that the Council has which involves a third party processing personal data on its behalf must be set out in writing in a Data Processing Agreement (DPA). Whilst a signed DPA was in place for SEEMiS, it was noted that two secondary schools have purchased a separate school management software package which is being used by them for tracking and monitoring purposes instead of SEEMiS. The Service has agreed to complete a data protection impact assessment (DPIA) on the use of the system and depending on the outcome, either cease its use or establish a DPA with the supplier.

1. INTRODUCTION

1.1 Strathclyde Educational Establishments Management Information System (SEEMiS) is used by all Scottish Councils to support electronic education administration within Council headquarters and schools.

1.2 SEEMiS is a Limited Liability Partnership (LLP) made up of all Scottish Local Authorities, including Aberdeen City Council. There is a Board of Management, containing both Council Officers and Elected Members, which acts on behalf of the member authorities. In 2014, SEEMiS introduced geographical Customer Account Managers as a point of contact for Local Authorities. There are also a number of user groups where representatives from each area discuss current issues.

1.3 SEEMiS provides the management information needs of all Aberdeen City Council schools as well as a wide range of central administrative and quality improvement functions. It is used for the maintenance of personal and academic (including SQA) records for pupils; personal information and work records for staff; and attendance records for pupils and staff.

1.4 The objective of this audit was to provide assurance that appropriate control is being exercised over the system in view of the perceived criticality of the system and the significant volume of sensitive personal data held.

1.5 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Eleanor Sheppard, Chief Education Officer, Shona Milne, Quality Improvement Manager, and Charlie Love, Quality Improvement Officer.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Procedures

2.1.1 Comprehensive written procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance of correct and consistent practices being followed, especially in the event of an experienced employee being absent or leaving.

2.1.2 Online system guidance notes are provided by SEEMiS on their website which can be accessed by anyone with a SEEMiS username. There are also Council specific "how to" guides available on the Council's intranet. In addition, schools are able to contact the Council's Management Information System (MIS) Support team, regarding any queries / issues and if required this can be escalated onwards to the software supplier's help desk. In the school year August 2018 to July 2019, over 3,000 calls were received by the MIS Support Team of which 396 calls were passed onwards to the software supplier.

2.1.3 The Council does not have any corporate procedures relating to what level of access should be provided to which staff role. This has been delegated to a school level as the staff roles at each school can vary considerably. The MIS Support team has prepared Corporate profile access templates on the system to assist schools but in the majority of cases schools will amend them as appropriate.

2.2 User Access

2.2.1 SEEMiS is used to manage pupil personal data along with their progress through the curriculum. It also manages school staff personal details to allow group emails and text messaging to be issued to all staff, as well as enabling teaching staff to be allocated to the classes they will be teaching. This requires all staff to be set up as a staffing record on the system, which automatically allocates them a username and password, even though they may never require to access the system, e.g. janitors, children's escorts, etc. Once the staffing record has been completed, which covers personal details, a work record will be created detailing the position they are filling at the school, e.g. Head Teacher (HT) Principal Teacher (PT), Teacher, support staff. As some staff may fill more than one role within the school, they may have more than one work record, e.g. PT and Teacher, or Teacher (Geography) and Teacher (History).

2.2.2 Once the staff record has been created, a profile will be assigned which dictates the screens and reports within SEEMiS that the member of staff will be able to access. Further access rights will be allocated detailing no access, view access, or edit access of pupil records and a role responsibility setting, which will dictate whether they can access pastoral notes (guidance teacher notes) or reasons for absence

2.2.3 Access to the system should be commensurate with an employee's position, with users given a profile to either view or edit data to various levels. School specific user access is administered by administration staff within each school, with the MIS Support team at Marischal College responsible for administering all other users.

2.2.4 SEEMiS access and removal requests are processed through the MIS online service portal accessed through the Council's intranet. These are currently used for non-school based staff or those requiring access to the Tracking and Monitoring module (described in paragraph 2.2.5). However, at a school level this is managed by school system administrators and the majority of access is set up based on verbal requests by the school's senior management team. This means there is no documented approval process to support the level of access being granted to staff within schools.

Recommendation
Education should introduce a documented approval process for providing access at a school level.

Service Response / Action
Agreed. The Service will develop a documented process for the creation and management of SEEMiS accounts.

Implementation Date	Responsible Officer	Grading
April 2020	Quality Improvement Officer	Significant within audited area.

2.2.5 Teachers are able to access the Tracking and Monitoring module of SEEMiS from home using their personal computers. This is mainly used to allow pupil reports to be written at home. Access is via the SEEMiS website using the same username and password as used on a Council computer. Home access has to be specifically set up for the user and a memorable word is required as a secondary password before access will be granted to the system.

2.2.6 A major system upgrade is scheduled for the system which will mean staff can access all the main modules from personal ICT devices, not just Council provided devices. Local authorities are expected to be able to retain the option of only allowing access on Council ICT devices. Should the Council opt for access from personal ICT devices the importance of effective access control by schools, to avoid unauthorised access to the system and the personal data it holds, will increase.

2.2.7 The list of SEEMiS users in November 2019 was reviewed against a list of leavers extracted from the payroll system. This matching process found 58 leavers within 23 schools who still had current "work records" within SEEMiS (user names) of which 30 had their accounts locked (accounts will be locked after 100 days of inactivity or 3 incorrect password attempts). The breakdown of these leavers by year with current work records was as follows: 2015 - 1, 2017 - 3, 2018 - 38 and 2019 - 16. When a member of staff leaves an establishment, an end date should be recorded against their work record on SEEMiS which removes their ability to access the system.

Recommendation
a) SEEMiS accounts for former school employees should be disabled.

b) Schools should be informed that an end date should be recorded in SEEMiS against any staff member leaving a school in a timely manner.

Service Response / Action
a) Agreed. The Service will review current accounts and instruct schools to remove work records for staff no longer in post.

b) Agreed. The setting of an end date will be addressed in updated procedures for schools.

Implementation Date	Responsible Officer	Grading
April 2020	Quality Improvement Officer	Significant within audited area.

2.2.8 Users should only be able to access information for the school to which they are assigned. There are cases, however, where staff require access to more than one school. Ten SEEMiS users with access to more than one school were reviewed for reasonableness.

Five were visiting specialist teachers covering an area of schools and three held part time positions at more than one school. The remaining two teachers still had access to SEEMiS for schools within which they were no longer employed.

2.2.9 The MIS Support team is not notified when staff who have access to the system leave the Council, therefore they aim to conduct an annual review of all non-school based staff with SEEMiS access and remove those who no longer require it. The last review was undertaken in August 2019.

2.2.10 A review of the current user profiles found 111 differently named profiles which were spread across 109 job roles (per the payroll system). Unfortunately, SEEMiS reporting cannot provide the detail of which screens and fields each of these profiles has access to, nor does it show the access rights to the pupil records, and responsibility settings for some of the modules.

2.2.11 Based on the findings in paragraph 2.2.7, describing SEEMiS accounts remaining current for former school employees, it would appear that an annual user audit of school staff access to SEEMiS, is not undertaken. All schools are required to undertake an annual ScotXed census return in September. An annual audit would assist in identifying any former employee SEEMiS accounts which were not disabled and if done at the ScotXed return time should not cause additional work for staff. It would also be an opportunity to review profiles allocated to staff to ensure they are commensurate with their role and duties within the school.

Recommendation
The Service should consider introducing a regular review of all SEEMiS users and their access levels.

Service Response / Action
Agreed. An updated process will be established to manage access requests and provide assurance that staff no longer employed are removed from the system.

Implementation Date	Responsible Officer	Grading
April 2020	Quality Improvement Officer	Significant within audited area.

2.3 Password Security

2.3.1 Access to SEEMiS is granted via a username and password. The system's password guidance requires that passwords be a minimum of eight characters, should incorporate a combination of lower and upper case characters, and numbers. Symbols are considered optional to increase complexity. The guidance also currently requires that passwords should be changed at least every ninety days and the same password cannot be re-used within five successive changes.

2.3.2 The SEEMiS password requirements are in accordance with the Council's ICT Access Control Policy and accompanying Password Standard.

2.3.3 User accounts lock after three incorrect password attempts, at which point users must contact the school's system administrator to have their password reset and account unlocked. System administrators are able to run a report within their establishment, should it be required, which shows all users and information on when they last logged in, last failed login, how many failed logins they've had, and whether the account is locked.

2.4 Data Protection

2.4.1 All Council employees are required to comply with the Council's Corporate Information Policy and Managing Information Handbook, which covers staff responsibilities in relation to data protection. Mandatory Information Governance training became available on the Council's online interactive learning (OIL) platform in July 2018. A report provided by People and Organisation showed that, as at 30 November 2019, there were 391 permanent staff and 544 relief staff within Integrated Children's and Family Services who had not completed this mandatory training.

2.4.2 A comparison of current SEEMiS users with the list of those staff who had not completed the training as at 30 November 2019, identified 362 current users who had not completed the training. As SEEMiS holds personal information about both pupils and staff, if staff have not completed the required Information Governance training, there is an increased risk staff processing personal data will be unaware of their responsibilities under data protection legislation.

Recommendation
The Service should ensure that all staff who have access to SEEMIS complete the Information Governance training

Service Response / Action
Agreed. The Service will instruct those still to complete the Information Governance training to do so. The requirement to complete this training will be considered as part of the new access procedure.

Implementation Date	Responsible Officer	Grading
June 2020	Quality Improvement Officer	Significant within audited area.

2.4.3 Under Data Protection legislation, the Council is required to ensure that all personal data processed is adequate, relevant and limited to the purposes for which it is processed. When reviewing the information required to set up a user account, it was noted that staff personal data, including date of birth, marital status, and National Insurance number is collected. The MIS Support team has advised that this information is based on the mandatory information required by the system and whilst the system will accept "unknown" in the marital status field, the others require to be completed. These details are not required to set up user accounts in other Council systems which hold personal data (e.g. Benefits or Housing rents).

Recommendation
The Service should discuss the user account requirements (specifically National Insurance and Marital Status) with SEEMiS to ascertain the reason why this personal data is collected and if appropriate request a system revision to remove the mandatory requirement for this data.

Service Response / Action
This information is currently mandatory within SEEMiS as the product has an HR function within some local authorities. This request for a system revision has been passed to SEEMiS via our account manager for consideration in the design of the new SEEMiS Schools product which is scheduled for release in January 2021.

Implementation Date	Responsible Officer	Grading
Implemented	Quality Improvement Officer	Significant within audited area.

2.4.4 In accordance with the Council's Managing Information Handbook and in order to comply with data protection legislation, any arrangement that the Council has which involves a third party processing personal data on its behalf, such as the arrangement with SEEMiS, must be set out in writing in a Data Processing Agreement (DPA), either as part of the contract with the supplier or as a standalone agreement. The DPA should be drafted with the support of Governance following completion of a Data Protection Impact Assessment and should be signed off by a Proper Officer in Governance on behalf of the Council's Monitoring Officer. In addition, the DPA should record: the subject matter and duration of the processing; nature and purpose of the processing; type of personal information and categories of data subject; obligations and rights of the Council as controller and processor (SEEMiS); and security arrangements in respect of the processing.

2.4.5 A Service Agreement between the Council and SEEMiS was signed in September 2016 covering data protection and confidentiality along with a Service Agreement variation covering GDPR requirements signed in December 2018. The original contract and variation were signed by Proper Officer from Governance and addressed the DPA requirements detailed in paragraph 2.4.4.

2.4.6 Two secondary schools have purchased a separate school management software package which is being used by them for tracking and monitoring purposes instead of SEEMiS. The software supplier is processing personal data on behalf of these schools. When the schools were contacted, they were unable to provide a signed DPA with the supplier.

Recommendation

a) A Data Protection Impact Assessment should be completed for the use of the alternative management information system.

b) A Data Processing Agreement should be established with the supplier.

Service Response / Action

a) Agreed. A DPIA is already being progressed for the OnTheButton system and is awaiting further information from the supplier.

b) Following the completion of the DPIA the use of the OnTheButton system will be reviewed and a Data Processing Agreement will be put in place if use of the system is to continue.

Implementation Date	Responsible Officer	Grading
April 2020	Quality Improvement Officer	Significant within audited area.

2.4.7 SEEMiS transfers personal data which the Council controls to: the SQA; the Scottish Government; Skills Development Scotland; and the Council's online course and revision provider. In addition, a number of staff from the NHS, Police Scotland and the Council's pupil mentoring provider have access to personal data on SEEMiS.

2.4.8 Where the Council is carrying out routine internal or external personal data sharing on a regular basis or where the Council reasonably expects to carry out personal data sharing on an ad-hoc basis with a third party, an Information Sharing Agreement should normally be put in place with the third party, to ensure good governance around the arrangement. Alternatively, a Memorandum of Understanding may be put in place to set out an agreed information sharing approach at a higher level.

2.4.9 All new information sharing arrangements should be assessed under the Council's Data Protection Impact Assessment (DPIA) process. This will normally require a DPIA, to

enable issues and risks to be identified in relation to compliance with data protection legislation and to identify areas which should be addressed through the Information Sharing Agreement. All Information Sharing Agreements must be signed off by the proper officer in Governance prior to being added to the Council's Information Sharing Protocol register and then being published on the Data Protection page of the Zone. At the time of the audit a DPIA had yet to be completed for SEEMiS.

2.4.10 Data sharing agreements are in place with organisations who have access to SEEMiS data. However, Education advised the agreement with the SQA is historic and was unavailable for review at the time of the audit. By completing a DPIA, this will highlight all the organisations who currently access information held on SEEMiS and enable the Cluster to ensure the required data sharing agreements are in place.

Recommendation

a) The Service should assess whether a Data Protection Impact Assessment is required for SEEMiS, in conjunction with the Data Protection Officer.

b) The Service should ensure data sharing agreements are in place which cover current routine sharing of personal data with third parties.

Service Response / Action

a) Agreed.

b) Required Data Sharing Agreements will be developed where not in place.

Implementation Date	Responsible Officer	Grading
September 2020	Quality Improvement Officer	Significant within audited area.

2.5 Contingency Planning and Disaster Recovery

2.5.1 Any query in relation to the use of SEEMiS is initially referred to the MIS Support helpdesk, and if it cannot be resolved it is then referred to SEEMiS for further assistance. Digital and Technology staff would only become involved if there is a local problem accessing SEEMiS, such as in relation to internet connectivity.

2.5.2 Data is currently backed up on a daily basis in two data centres: one at the South Lanarkshire Council Data Centre in Hamilton, the other at the Scottish Government Data Centre in Edinburgh. SEEMiS has included their Business Continuity Plan within the Service Agreement they have with Councils.

2.5.3 SEEMiS advised that they perform disaster recovery testing with consideration of the benefits (in terms of assurance gained) and the related risk of disruption to operational services, undertaking such testing based on operational need. Education confirmed that they are advised of such site level disaster recovery testing when it is carried out e.g. the disaster recovery testing invoked in October 2018 when the supplier migrated to a new data centre. The system supplier acknowledges that the decision not to undertake regular, scheduled site level disaster recovery testing does lead to a level of residual risk, albeit this is considered low.

2.5.4 The system supplier also advised that they obtain further assurance on disaster recovery arrangements as part of monthly patching of servers and by monitoring system back-up success.

2.5.5 Should SEEMiS become unavailable during school opening hours this impacts on schools' ability to carry out pupil registration, which allows schools to track pupils and instigate

processes when any pupil fails to be registered as expected. If a system outage occurs at the beginning of the school day, teachers will be issued paper registers on which to carry out the process, and these will be passed to administration staff for checking and to follow up on unaccounted for pupils. Access to contact details is provided through the paper census forms that are completed by parents at the beginning of each school year. The same documents provide any serious medical conditions that might affect a pupil.

AUDITORS: D Hughes
A Johnston
G Flood

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.