The Highland Council
Comhairle na
Gàidhealtachd

# INTERNAL AUDIT
# FINAL REPORT

## ORKNEY ISLANDS COUNCIL

## SEEMiS EDUCATION MANAGEMENT INFORMATION SYSTEM

| AUTHOR | DISTRIBUTION |
|---|---|
| David Beaton | Executive Director of Education, Leisure and Housing |
| IT Auditor | Executive Director of Corporate Services |
| Internal Audit | Head of Schools |
| Finance Service | Head of Buildings and Facilities |
| Highland Council | Educational Resources Manager |
| | Senior Administration Officer |
| | IT Support Supervisor (Education and Recreation) |

**DRAFT DATE: 06/08/15**
**REF:** OIC01/001.bf          **FINAL DATE: 15/09/15**

## **Contents**

## 1.   INTRODUCTION

The purpose of this report is to record the findings of a recently completed audit review in respect of the Education Management Information System (MIS) known as SEEMiS.

SEEMiS is a web based system which is hosted in Hamilton and is now used by all 32 Scottish Councils. Originally formed by twelve of the ex-Strathclyde Councils, SEEMiS delivers an MIS to all sectors of the Scottish education system. In July 2010, the organisation became a Limited Liability Partnership (LLP) wholly owned and managed by the then 28 member councils. In 2014 the remaining 4 Scottish councils also became members of SEEMiS. Hence the system is now used by all Scottish councils.  SEEMiS is governed by a Board of Management, containing both council officers and elected members, which acts on the behalf of the member councils.

SEEMiS contains a large number of modules which are used to carry out different functions including the following:

- Click and Go - the integrated school management system
- Tracking, Monitoring and Reporting – used to track pupil attainment and effort, homework and behaviour
- Pastoral Notes
- EMA Management – manages all aspects of education maintenance allowance payments
- Clothing grants and free school meals
- Staff Absence and Appointment
- Supply Staff Booking

There is also a web enabled version of Click and Go that allows a limited amount of pupil information to be accessed over the internet by teachers working away from the school.

SEEMiS contains personal details of teachers in addition to both personal and sensitive personal details of pupils as defined by the Data Protection Act.  Personal data loss of this nature has previously resulted in substantial fines from the Information Commissioner's Office (ICO) in other UK councils.  Therefore the security of the system is important.

## 2.   REVIEW OBJECTIVES

The objectives of the review were to ensure that:

(i)     Access to the system is adequately controlled

(ii)    System, pupil and staffing data input is complete, accurate and up to date

(iii)   Interface processing to and from other systems is properly checked and reconciled

(iv)    Sufficient management and data quality reports are produced, securely distributed and then disposed of when no longer required

(v)     The electronic audit trails are properly set up and maintained

(vi)    License and support arrangements comply with expected best practice

(vii)   The system operates both efficiently and effectively.

### 3. SCOPE, METHOD AND COVERAGE

The following information relating to the system was examined:

- Modules within the SEEMiS System and its associated interface programs
- The Education policy and procedures relating to schools, staff and pupils
- All paper records associated with SEEMiS processing and system administration
- The Council's polices relating to data protection and information security

The following standards and best practice were also referred to:

- The Institute of Internal Auditors Information Systems Auditing Manual
- The information security standards ISO 27001 and ISO 27002.

Meetings were held with the following staff to discuss the operation of the system:

- SEEMiS System Administrator
- IT Support Supervisor (Education and Recreation)
- Educational Resources Manager
- School Business Managers
- Depute Head

Thanks are extended to all of these officers for their courtesy, co-operation and assistance in this assignment.

### 4. MAIN FINDINGS

The main findings of the review, referenced to the above review objectives, are as follows.

### 4.1 Access Control

Objective (i) was only partially achieved.

To prevent unauthorised access to personal pupil and teacher data on SEEMiS the expected controls are:

a) An Access Control Policy is used to define user access controls and is adhered to by system administration staff responsible when they set up user access.

b) A formal User Registration System is used to ensure that all users who are given access to the system have their access to the system formally recorded and authorised.

c) User access is reviewed at least once per year to ensure access levels are correct.

d) Passwords used to access the system have enforced complexity to ensure they are not easily guessable.

e) Users are timed out of the system after a specified period, e.g. one hour, if they have logged into it, but do not then use it.

f) Users are disabled after a specified period, e.g. six months, if they are set up to access to the system, but do not then log into it.

g) Staff using the SEEMiS system should have carried out information security training so they are aware of the Council's information security guidance.

h) Equipment used to access the SEEMiS System is encrypted to ensure that any data extracted from the SEEMiS system onto this equipment is protected from unauthorised access in the event that the equipment is lost or stolen.

With reference to the above controls, the corresponding findings were:

a) A draft Access Control Policy does exist but it needs to be improved to cover all areas including administration staff and school technicians. Then it needs to be formally approved for use and system administration staff members need to adhere to it when setting up user access.

b) The users accessing the system and the access levels they have are not reviewed annually. A review of access levels during the audit found school technicians in a secondary school had been allocated an inappropriate level of access. This finding highlights the need for the annual review.

c) A formal User Registration System has been set up. All school employees are entered into SEEMiS and given a work record when they commence employment in a school. This, in turn generates a SEEMiS user name. Although each school employee is allocated a SEEMiS username, not all school employees are actually given access to SEEMiS.

d) Password complexity is not yet in place, but the system administrator has emailed SEEMiS to get it activated

e) Users are not currently timed out of the system after a specified period if they have logged into it but do not use it.

f) Users are not disabled after a specified period if they are given access to the system, but do not log into it. The SEEMiS supplier advised this facility can be configured if requested. For temporary staff, the SEEMiS supplier advised that user access is revoked automatically when the user's associated work record expires. However this timeout does not apply to permanent staff members who do not use the system.

g) The Council provides online training on information security for its staff. However there is no monitoring procedure to provide assurance that staff members have undertaken the training which means the number of school employees who have undertaken the training is unknown. Keys to school cabinets containing paper based pupil records are not always properly controlled and examples were identified during the review of keys either being left in the cabinets themselves of being stored in unlocked drawers overnight. This means that school staff such as janitors or cleaning staff who have access to the rooms containing these cabinets also have unrestricted access to these records.

h) Teachers need to be able to work securely on personal and sensitive data away from school as part of their conditions of employment. The personal and sensitive data worked on includes school reports, reports for children with identified needs, e.g. autism, dyslexia, etc. If personal pupil information is encrypted, it is regarded as being held securely by the ICO. If an encrypted PC or laptop is lost or stolen it does not need to be reported to the ICO. However the majority of the school PCs/laptops are not encrypted. Instead teachers have been provided with encrypted pen drives. Teachers have reported, however, that the existing pen drive encryption solution is difficult to use and have forgotten passwords. Evidence was found of at least one PC containing personal pupil information - the pupil tracker spreadsheets in St Andrews primary. The best way to ensure school PCs/laptops which are used by teachers to access pupil information are secure is to encrypt them. PCS/laptops which

are used for teaching purposes and do not contain personal information do not need to be encrypted.

**4.2    Data Input**

Objective (ii) was mainly achieved. The types of data input into SEEMiS include the following:

- Pupil enrolments
- Teacher contracts
- Pupil attendance
- Education maintenance allowances
- Clothing grants and free school meals
- Scottish Qualifications Authority exam results

Some of the SEEMiS data is checked as part of the various censuses carried out by ScotXed (Scottish Exchange of data).  The ScotXed Unit is part of Education Analytical Services Division within the Learning and Justice Directorate of the Scottish Government.  The censuses check the following data:

- The school establishments within the council
- Staff data in each school
- Pupil data in each school
- Pupil attendance, absence and exclusion data

In order to complete the ScotXed censuses, schools send the information they hold about each pupil to their parents/guardians annually and ask them to verify it is correct.  These surveys help to ensure that pupil data is correct, complete and up to date.

The following two concerns were identified during the review:

1) A sample check of pupil absence data found that the "To Be Confirmed" (T) absence indicator is not always being updated when the reason for the absence was established.  This means that absence information and census returns to ScotXed may be partially incorrect.

2) SQA exam records dating from 1968 to 1985 were found in a locked store-room in Stromness Academy.  The Council retention guidance provided for review of this type of information is current year plus 6 years.  Hence this personal information is being retained for longer than is necessary and is not in accordance with the Data Protection Act.

**4.3    Interface Processing**

Objective (iii) was also mainly achieved.  Data is extracted from and loaded into SEEMiS for a number of reasons.  These include the following:

- As mentioned above, school, teacher and pupil data is extracted from SEEMiS and sent to ScotXed as part of the various censuses carried out by ScotXed

- Exam registrations, entries and results are extracted and electronically transmitted to the Scottish Qualifications Authority (SQA) and returns from the SQA are loaded into SEEMiS

- Education Maintenance Allowance BACS payment files are extracted from SEEMiS and transferred to the banks via the Council's BACS software

One area of concern was identified.  A review of a sample of EMA payments identified that a few EMA payments do not seem to be in accordance with the EMA guidance.  The EMA guidance provided by the Scottish Government states that:

*"EMA is a weekly allowance requiring 100% attendance at all timetabled sessions. Part payments for part attendance will not be made"*

However examples were found where the system seemed to state that 100% attendance had been achieved during the week but the pupil had not been paid. In addition, instances were found where 100% attendance had not been achieved but the pupil had been paid.  Although a note field is provided to explain the reasons for payments and non-payments no notes existed to explain these occurrences.

## 4.4  Management and Data Quality Reports

Objective (iv) was partially achieved.  The expected control was that a list of management and data quality reports would have been available for review to provide assurance that all the required management and data quality reports have been identified and produced.

The finding was that no such list is available for review. Some management and data quality reports have been developed and details of these are available. However, as identified above, the "To Be Confirmed" (T) absence indicator is not always being updated and a data quality report has not been developed to identify this problem.

## 4.5  Audit Trail

Objective (v) was achieved.  The following modules have electronic audit trails set up to audit the update of financial transactions:
- Clothing, grants and free school meals
- Education Maintenance Allowance Payments.

There is also an audit trail showing when users have logged into SEEMiS.

## 4.6  License and Support

Objective (vi) was partially achieved.  A Memorandum of Understanding exists between Orkney Islands Council and South Lanarkshire Council and the SEEMiS Group LLP was provided for review.  However the SEEMiS supplier has advised this is out of date. The supplier stated the member councils currently have the new, approved by the AGM, 'Members Agreement'.  This Agreement covers the use of SEEMiS software.  It was not provided for review during the audit.  A new Services Agreement is currently with the supplier's lawyers.  It will be passed to the SEEMiS Board in September 2015 for approval and subsequent issue.

## 4.7  Performance

Objective (vii) was partially achieved. The various SEEMiS modules are being widely used throughout the Council. However three concerns relating to efficiency were identified:

1) All staff involved in the audit reported persistent problems with the performance of SEEMiS and some of these problems were present during the review.  They included very poor response times, numerous error messages appearing and the system not being available for use.   These problems are frustrating for staff and contribute to inefficiency.  The poor performance is a known problem and a member of the IT Unit has stated that an improved network link is to be introduced which is hoped will address it.

2) There is double entry of teacher's contract details into both the Northgate HR/Payroll System and SEEMiS.  Although the same data should be held in both systems no reconciliation takes place to provide assurance that this is the case.  Double entry of the same information is an inefficient use of staff time..

3) Parts of the SEEMiS are not being used.  The reasons are follows:

- Because of SEEMiS performance issues and SEEMiS not being available for a prolonged period, St Andrews Primary School use pupil tracker spreadsheets instead of the pupil tracker facility in SEEMiS.  However the SEEMiS pupil tracker facility operates in Stromness Academy and is used for report cards.

- Kirkwall Grammar School (KGS) use a separate School Management System called OnTheButton for pupil pastoral notes because they find it is more efficient. The functionality provided by this system duplicates some of the functionality provided by SEEMiS, so the Council is paying twice for software.  It was reported that the OnTheButton server is not supported by the IT Unit during the visit to KGS and it was not possible at that time to establish how the system is backed up.

- Staff absences are not recorded on SEEMiS but on spreadsheets instead.  SEEMiS has a facility to record staff absence but it is not being used.

The SEEMiS software license cost the Council approximately £23,700 in 2014/2015 and it is important to analysis its use to provide assurance that it is being used efficiently.

## 5.    CONCLUSION

It was pleasing to find that many of the expected controls are already in place.  User access is both administered and controlled.  Access levels reflect staff duties.  There are checks carried out that both data input and interface processing are complete and correct.  Data quality reports are being developed and financial transactions are audited.

Nevertheless some of these control areas still need further improvement to approach best practice.  The most important required improvement is considered to be the provision of adequate IT facilities to allow teachers to work securely away from the school, e.g. at home.  Although encrypted pen drives are provided, teachers have reported difficulty in using them.

The review made six recommendations, one at high priority and five at medium priority.  All are due to be complete by 31 March 2016.

## 6.    AUDIT OPINION

The opinion is based upon, and limited to, the work performed in respect of the subject under review.  Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist.  It is the opinion that **Reasonable Assurance** can be given in that whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.    The levels of assurance and their definitions can be found at Appendix 1.

## 7. ACTION PLAN

The Action Plan contains **6** recommendations as follows:

| Description | Priority | Number |
|---|---|---|
| Major issues that managers need to address as a matter of urgency. | High | 1 |
| Important issues that managers should address and will benefit the Organisation if implemented. | Medium | 5 |
| Minor issues that are not critical but managers should address. | Low | 0 |
| **Total recommendations** | | **6** |

| REPORT REF. | PRIORITY | FINDING | RECOMMENDATION | MANAGEMENT AGREED ACTION | IMPLEMENTATION RESPONSIBLE OFFICER | TARGET DATE |
|---|---|---|---|---|---|---|
| 4.1 | High | **Access Control** | | | | |
| | | a) A draft Access Control Policy does exist but it needs improved and approved. | a) The draft Access Control Policy needs to be improved to cover all types of users including administration staff and school technicians. Then it needs to be formally approved for use and system administration staff members need to adhere to it when setting up user access. | a) Policy to be improved then formally approved and distributed to appropriate staff members in schools. | Senior Administration Officer | 31/12/15 |
| | | b) The users accessing the system and the access levels they have are not reviewed annually. A sample check during the audit found school technicians in KGS had a high level of access and could access pupil records which was incorrect. | b) User access should be reviewed annually and any required corrections or updates should be carried out. | b) Reviewed at time of Staff Census. | Senior Administration Officer | 31/10/15 |
| | | c) Password complexity is not yet in place. | c) Password complexity should be activated. The system administrator has emailed SEEMiS to get this done | c) Request update from SEEMIS on timescale for this. | Senior Administration Officer | 31/10/15 |

| REPORT REF. | PRIORITY | FINDING | RECOMMENDATION | MANAGEMENT AGREED ACTION | IMPLEMENTATION | |
|---|---|---|---|---|---|---|
| | | | | | RESPONSIBLE OFFICER | TARGET DATE |
| | | d) Users are not disabled after a specified period if they are given access to the system but do not log into it. | d) SEEMiS should be asked to supply a time out facility to log out users who have logged into the system, but not used it for a specified period of time, e.g. an hour | d) Investigate one hour recommendation with SEEMIS | Service Improvement Officer/Senior Administration Officer | 31/10/15 |
| | | e) Users are not disabled after a specified period if they are given access to the system but do not log into it. For temporary staff SEEMiS have advised that user access is revoked automatically when the user's associated work record expires. However this timeout does not apply to permanent staff members who do not use the system, but do not log into it. SEEMiS have advised this facility can be configured if requested. | e) SEEMiS should be asked to provide the facility to automatically disable users who never logged into the system after a specified period of time, e.g. 6 months | e) This has been investigated further with SEEMIS who have confirmed that the automatic process is not available. However access will be disabled for those staff who no longer require to use the system on an annual basis. | Service Improvement Officer/Senior Administration Officer | 31/10/15 |
| | | f) OIC provides online training on information security for its staff. However there is no monitoring procedure to provide assurance that staff members have undertaken the course which means the number of staff in schools who have undertaken the training is unknown. | f) Reports should be provided to all head teachers showing who has completed the training in the school. In addition face to face training should also be considered for selected staff in schools as it would have more impact on the substantial financial risks of losing personal pupil data. | f) Reports to be requested | Senior Administration Officer | 31/10/15 |
| | | g) Keys to school cabinets containing paper based pupil records are not always properly | g) The control of school keys should be reviewed to ensure | g) Schools to be reminded of data security | Educational Resources Manager | 31/10/15 |

| REPORT REF. | PRIORITY | FINDING | RECOMMENDATION | MANAGEMENT AGREED ACTION | IMPLEMENTATION | |
|---|---|---|---|---|---|---|
| | | | | | RESPONSIBLE OFFICER | TARGET DATE |
| | | controlled and examples were identified of keys either being left in the cabinets themselves of being stored in unlocked drawers overnight. This means that school staff such as janitors or cleaning staff who have access to the rooms containing the cabinets also have unrestricted access to these records | that keys to cabinets containing pupil information are only accessible to authorised staff, e.g. teachers and school office staff. | | | |
| | | h) If personal pupil information is encrypted, it is regarded as being held securely by the ICO and if an encrypted PC or laptop is lost or stolen it does not need to be reported. However the majority of the school PCs/laptops are not encrypted. Instead teachers have been provided with encrypted pen drives. Teachers have reported, however, that the existing pen drive encryption solution is difficult to use and they have forgotten their passwords on occasion. Evidence was found of at least one PC containing personal pupil information. | h) A review of the use of encryption should be carried out with a view to improving security. The following as measures should be considered:<br><br>• The provision of encrypted equipment for senior staff, guidance teacher and assisted learning teachers who all access sensitive pupil information<br><br>• Having a pool of encrypted laptops in each school to allow home working for teachers<br><br>• How to allay the existing teacher concerns with regard to the existing pen drive arrangement<br><br>• Allowing all teachers who | h) A reminder will be issued to all schools to remind staff that personal data should not be held on unencrypted PCs/laptops and guidance shall be issued on the use of encrypted pen drives.<br><br>Full Encryption Solutions for all staff machines to be investigated. This will have funding and installation resource implications.<br><br>Completion date for full implementation dependant on funding and resources | Educational Resources Manager<br><br>IT Support Supervisor (Education and Recreation) | 31/10/15 |

| REPORT REF. | PRIORITY | FINDING | RECOMMENDATION | MANAGEMENT AGREED ACTION | IMPLEMENTATION | |
|---|---|---|---|---|---|---|
| | | | | | RESPONSIBLE OFFICER | TARGET DATE |
| | | | want to work from home to access their email from home. | | | |
| 4.2 | Medium | **Data Input**<br>1) The "To Be Confirmed" (T) absence indicator is not always being updated which means that absence information and returns to ScotXed may be incorrect.<br><br>2) Old SQA records were found in a Stromness Academy storeroom which should have been securely disposed of. | 1) A data quality report should be produced to identify occurrences of the "T" indicator to ensure they are timeously updated.<br><br>2) The old SQA records should be securely disposed of. | 1) Data checks to be carried out on monthly basis.<br><br>2) SA to be contacted and ensure records are securely disposed of in accordance with the OIC Data Retention Policy | Senior Administration Officer<br><br>Educational Resources Manager | 31/10/15<br><br><br><br><br>31/10/15 |
| 4.3 | Medium | **Interface Processing**<br>Examples were identified where the system seemed to state that 100% attendance had been achieved during the week but the pupil had not been paid. In addition, instances were found where 100% attendance had not been achieved but the pupil had been paid. | Sample checking of EMA payments should be carried out across secondary schools to ensure the payments are consistent with the national guidance. | Sample checking to be carried out on monthly basis | Senior Administration Officer | 31/10/15 |
| 4.4 | Medium | **Management and Data Quality Reports** | An exercise should be carried out | Identify management | Senior | 31/12/15 |

| REPORT REF. | PRIORITY | FINDING | RECOMMENDATION | MANAGEMENT AGREED ACTION | IMPLEMENTATION | |
|---|---|---|---|---|---|---|
| | | | | | RESPONSIBLE OFFICER | TARGET DATE |
| | | Some management and data quality reports have been developed. However the "To Be Confirmed" (T) absence indicator is not always being updated which means that absence information and returns to ScotXed may be incorrect. A data quality report has not been developed to identify this problem. | to identify all the management and data quality reports that are required. These reports should both provide performance information and <u>evidence</u> that the data held within SEEMiS is complete, correct and up to date. | and data quality reports required, implement system for carrying out checks and collecting evidence to ensure data is complete, correct and up to date. | Administration Officer | |
| 4.6 | Medium | **License and Support**<br>The Members Agreement covering the use of the SEEMiS software was not provided for review during the audit. | The Members Agreement should be found. | Agreement (dated 20/8/15) passed to Legal Services prior to signing. | Senior Administration Officer | 31/10/15 |
| 4.7 | Medium | **Performance**<br><br>1) All staff involved in the audit reported problems with the performance of the SEEMiS system. | 1) The performance problems and the effect of the improved network link should be monitored. If the problems persist further action should be taken. | 1) Investigating (waiting for SWAN link) | 1) IT Support Supervisor (Education and Recreation) | 31/10/15 |
| | | 2) There is double entry of teacher's contract details into both the Northgate HR/Payroll System and SEEMiS. | 2) An interface between the systems should be considered. How the contract information is used in each system should also be analysed to ensure there is no overlap. | 2) Investigate possibilities with SEEMIS and HR/Payroll | 2) Service Improvement Officer/Senior Admin Officer | 31/03/16 |
| | | 3) Parts of SEEMiS functionality are not currently being used. In addition the OnTheButton software duplicates part of the | 3) A review of the use of SEEMiS functionality should be carried out to identify whether the best value for money is being | 3) A review will be carried out on use of SEEMIS functions.<br><br>A review will be | 3) Senior Admin Officer<br><br>IT Support | 31/03/16<br><br><br>31/10/15 |

| REPORT REF. | PRIORITY | FINDING | RECOMMENDATION | MANAGEMENT AGREED ACTION | IMPLEMENTATION | |
|---|---|---|---|---|---|---|
| | | | | | RESPONSIBLE OFFICER | TARGET DATE |
| | | SEEMiS functionality. | obtained.   The usefulness of OnTheButton should be included within that review. The risks associated with the use of OnTheButton should also be reviewed. | carried out on the use of OnTheButton | Supervisor (Education & Recreation)/ Service Improvement Officer | |

**Internal Audit Opinion**

| Level | Definition |
|---|---|
| **Full Assurance** | There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied. |
| **Substantial Assurance** | While there is generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk. |
| **Reasonable Assurance** | Whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk. |
| **Limited Assurance** | Weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk. |
| **No Assurance** | Control is generally weak, leaving the system open to significant error or abuse, and/ or significant non-compliance with basic controls leaves the system open to error or abuse. |