27

|  |  |
| --- | --- |
| **HIGH LIFE HIGHLAND**  **REPORT TO BOARD OF DIRECTORS**  **11 December 2024** | AGENDA ITEM 8 REPORT No HLH/27/24 |

**FINANCE REPORT - Report by Chief Executive**

**Summary**

The purpose of this report is to update Directors on the financial performance of High Life Highland for quarter two 2024/25 and other relevant matters.

It is recommended that Directors:

1. note the draft year end outturn for 2024/25 as detailed in **Appendices A-C** reports a projected deficit of £247k;
2. note the breach of internal controls reported in the past quarter;
3. note no reportable data breaches have been reported in the past quarter;
4. note the internal audit report on HLH’s Data Protection processes at **Appendix E**;
5. note the award of contract at paragraph 7.1;
6. approve the internal audit recommendation to formalise the reporting requirements for data breaches;
7. approve the proposed three year audit plan; and
8. note the policy updates.

|  |  |
| --- | --- |
| **1.**  1.1 | **Business Plan Contribution**  High Life Highland’s (HLH) purpose is Making Life Better. The HLH Business Plan contains eleven Business Outcomes which support the delivery of this purpose, and this report supports all the outcomes from the Business Plan:   1. Seek to continuously improve standards of health and safety. 2. Commit to the Scottish Government’s zero carbon targets and maintain the highest standards in environmental compliance. 3. Use research and market analysis to develop and improve services to meet customer needs. 4. Increase employee satisfaction, engagement and development to improve staff recruitment and retention. 5. **Improve the financial sustainability of the company.** 6. Value and strengthen the relationship with THC. 7. Develop and deliver the HLH Corporate Programme and seek to attract capital investment. 8. Use research and market analysis to develop and deliver proactive marketing and promotion of HLH and its services. 9. Initiate and implement an ICT digital transformation strategy across the charity. 10. Develop and strengthen relationships with customers, key stakeholders and partners. 11. Deliver targeted programmes which support and enhance the physical and mental health and wellbeing of the population and which contribute to the prevention agenda. |

1. **Background**
   1. Directors of HLH receive a Finance Report on a quarterly basis. The primary purpose of the report is to summarise the financial performance of the charity and its subsidiaries.
   2. The financial content of this report has been scrutinised by the 11 November 2024 Finance and Audit Committee.

###### Financial Performance for Quarter 2 2024/25

* 1. The results for the period to September 2024 have been prepared. HLH’s consolidated financial performance for the period is summarised in **Appendix A**. The results for the period are further split by the 9 business categories in **Appendix B** and by cost category (income, staff costs and other costs) at **Appendix C**. Commentary on the performance of each service is provided in **Appendix D**.
  2. The draft outturn for the year to 31 March 2025 is a projected deficit of £247k with a negative variance to budget of £76k for income, £136k for Other Costs and £35k for staffing costs.
  3. The negative projected income variance is mainly due to lower than expected revenue in Museums & Galleries with café sales at North Coast Visitor Centre and Highland Folk Museum both forecast to be £30k below target, albeit partly mitigated by related savings in cost of sales. In addition, donations at Highland Folk Museum are projected to be £27k below budget and £10k lower than achieved in 2023/24.
  4. The North Coast Visitor Centre café was closed for 59 days this season due to sickness absence. Museum Attendant staff have been trained to work in the café to provide resilience in the catering operation going forward.
  5. Whilst visitor numbers at Highland Folk Museum increased 3.5% on the previous year, catering income has been impacted by poor weather in the early season in addition to issues in staffing the caterpod. The Museums team are developing an improvement plan for the new season to further improve customer numbers and increase donations.
  6. Income from the *high****life*** leisure membership scheme is virtually on target at the end of Q2 and projected to achieve budget at year end; however, it should be noted this is reliant on continued growth.
  7. As previously reported, the £136k projected pressure in Other Costs is due to the increase in Insurance Premium. Work is currently underway to try to reduce this for the following year. The staffing pressure in Facilities is due to additional posts required by increased operational requirements.
  8. Management actions are in place to reduce the projected deficit and bring the budget in on target.

|  |  |
| --- | --- |
| **4.** | **Pay Award 2024/25** |
| 4.1 | The CoSLA negotiated pay award for financial year 2024/25 has been finalised and implemented in November, backdated to 1 April 2024. |
| 4.2 | The award provides an uplift of £1,290 for employees earning up to £35k with all other employees receiving a 3.6% increase. |
| 4.3 | The annual revenue budget was calculated based on a 3% pay award with a corresponding uplift in the Service Fee as agreed with Highland Council. With the increase in wages higher than planned for, additional funding will be sought from Highland Council in accordance with the revised funding formula. |
| **5.** | **Internal Controls** |
| 5.1 | There was a salary overpayment of c. £20k identified in quarter two caused by a failure to submit the requisite paperwork. The incident is currently under investigation and an update will be provided at a future meeting. |
| 5.2 | The Head of Finance will provide an overview at the meeting on the current work being undertaken to deal with salary overpayments. |
| 5.3 | A breach of copyright occurred following the unauthorised use of an image by a member of staff. A financial settlement has been agreed with the claimant with refresher training and guidance also provided to staff. |
| **6.** | **Data Breaches** |
| 6.1  7.  7.1 | There have been no reportable data breaches reported in the last quarter.  **Tenders Approved/Contracts Awarded**  The following contract has been awarded:  QLM Ltd Health and Safety Consultancy Services Oct 24-Oct 27 |
| 8. | **Internal Audit** |
| 8.1 | The internal audit on HLH’s data protection processes was completed in October 2024 with an audit opinion of **Reasonable Assurance.** Jason Thurlbeck from THC’s Audit section will attend the meeting to discuss the findings of the audit. The report and resultant action plan is included at **Appendix E.** |
| 8.2 | Per recommendation M1 in the action plan, Directors are asked to agree that the current reporting arrangements for Data Protection are formalised with the notification of all data breach incidents reportable to the Information Commissioner’s Office. In addition, the results of the annual data protection audit will be presented to the Board. |
| 8.3 | The proposed three-year Internal Audit plan (2024-2026) for HLH under the SLA with The Highland Council covers the following three topics: |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Year | Audit Area | Scope | | | | |
| 2024 | Risk Management | Risk Management Process review   * Assessment against the IIA risk maturity model * Assess the management of two key risks | | | | |
| 2025 | Service provision -  Archives | Evaluate the effectiveness of processes and procedures to deliver and control service provision. Areas of focus:   * Requirements of the service delivery contract (SDC) * Service planning * Service delivery * Monitoring and reporting (within HLH and   additionally any reporting required by the SDC) | | | | |
|  | **Customer engagements** | **2021/22** | **2022/23** |  |
| Archives | 1,742,751 | 2,544,819 |  |
| 2026 | Leisure Management System (LMS) | A new Leisure Management System (LMS) is to be implemented in April 2025 to administer c.£12m of income p.a. The LMS will handle core leisure management functions.  The audit will identify the system objectives, risks and review its governance and high-level control framework. | | | | |

###### Policy Updates

* 1. In response to the THC Internal Audit on Data Protection detailed in paragraph 8, the existing Data Protection Policy has been updated to 1) expand the coverage to employees, volunteers and third-parties (it was previously limited to customers only); and 2) add in the ICO data protection ‘seven principles’ and detail the roles and responsibilities for data protection within the charity as recommended.
  2. The Risk Management Policy has been considered in line with the review schedule with no changes at this time.

###### Implications

* 1. Risk Implications – there are no new risk implications associated with the recommendations of this report.
  2. Equality Implications – there are no new equality implications associated with the recommendations of this report.
  3. Legal Implications – there are no new legal implications associated with the recommendations of this report.
  4. Resource Implications – there are no new resource implications associated with the

recommendations of this report.

**Recommendation**

It is recommended that Directors:

i.

ii. iii. iv.

v.

vi.

note the draft year end outturn for 2024/25 as detailed in **Appendices A-C**

reports a projected deficit of £247k;

note the breach of internal controls reported in the past quarter;

note no reportable data breaches have been reported in the past quarter;

note the internal audit report on HLH’s Data Protection processes at **Appendix E**; note the award of contract at paragraph 7.1;

approve

the

internal

audit

recommendation

to

formalise

the

reporting

requirements for data breaches;

1. approve the proposed three year audit plan; and
2. note the policy updates.

Designation: Chief Executive

Date 24 November 2024

Author: Neil Johnston, Head of Finance

37

###### Consolidated 2024/25: April to September APPENDIX A

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Budget** | **Actual (YTD)** | **Forecast (Year end )** | **Variance (Year End)** |
| Income | 35,931,214 | 16,415,234 | 35,855,354 | (75,860) |
| Staff Costs | (30,084,047) | (14,586,913) | (30,118,703) | (34,656) |
| Other Costs | (5,847,167) | (3,130,070) | (5,983,215) | (136,048) |
| **Surplus/(Deficit)** | **0** | **(1,301,749)** | **(246,564)** | **(246,564)** |

38

###### Variance by Sector APPENDIX B

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Budget** | **Actuals YTD** | **Forecast (Year end )** | **Variance (Year End)** |
| Adult | (721,859) | (405,245) | (704,733) | 17,126 |
| Archives | (746,343) | (322,842) | (721,881) | 24,462 |
| Facilities | (3,755,820) | (2,105,206) | (3,970,848) | (215,028) |
| Libraries | (3,680,974) | (1,771,198) | (3,680,917) | 57 |
| Management | (3,268,039) | (1,333,075) | (3,359,275) | (91,236) |
| Museums & Galleries | (1,096,734) | (517,311) | (1,136,037) | (39,303) |
| Music Tuition | (2,963,393) | (1,749,443) | (2,955,513) | 7,880 |
| Rangers | (502,670) | (182,442) | (485,800) | 16,870 |
| Sports | (807,762) | (358,837) | (800,699) | 7,063 |
| Youthwork | (1,866,745) | (879,320) | (1,841,200) | 25,545 |
| Service Fee | 16,646,339 | 8,323,170 | 16,646,339 | 0 |
| HC Financial Support | 2,764,000 | 0 | 2,764,000 | 0 |
| **Surplus/(Deficit)** | **0** | **(1,301,749)** | **(246,564)** | **(246,564)** |

39

###### Variance by Category APPENDIX C

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Income (£)** | | | | **Staff Costs (£)** | | | | **Other Costs (£)** | | | |
| **Budget** | **Actual**  **(YTD)** | **Forecast**  **(Year end )** | **Variance**  **(Year End)** | **Budget** | **Actual**  **(YTD)** | **Forecast**  **(Year end )** | **Variance**  **(Year End)** | **Budget** | **Actual**  **(YTD)** | **Forecast**  **(Year end )** | **Variance**  **(Year End)** |
| Adult | 172,874 | 52,688 | 172,874 | 0 | (813,144) | (414,438) | (796,018) | 17,126 | (81,589) | (43,495) | (81,589) | 0 |
| Archives | 294,206 | 179,662 | 309,148 | 14,942 | (997,827) | (484,900) | (996,370) | 1,457 | (42,722) | (17,604) | (34,659) | 8,063 |
| Facilities | 12,521,448 | 6,286,129 | 12,494,149 | (27,299) | (13,513,946) | (6,703,094) | (13,658,354) | (144,408) | (2,763,322) | (1,688,241) | (2,806,643) | (43,321) |
| Libraries | 49,559 | 25,037 | 53,867 | 4,308 | (3,188,005) | (1,499,086) | (3,173,354) | 14,651 | (542,528) | (297,149) | (561,430) | (18,902) |
| Management | 506,709 | 170,987 | 499,183 | (7,526) | (2,670,652) | (1,180,337) | (2,615,749) | 54,903 | (1,104,096) | (323,725) | (1,242,709) | (138,613) |
| Museums &  Galleries | 996,193 | 614,276 | 917,491 | (78,702) | (1,476,019) | (749,637) | (1,478,561) | (2,542) | (616,908) | (381,950) | (574,967) | 41,941 |
| Music Tuition | 593,801 | 22,695 | 598,855 | 5,054 | (3,113,687) | (1,506,897) | (3,113,826) | (139) | (443,507) | (265,241) | (440,542) | 2,965 |
| Rangers | 83,500 | 90,069 | 96,348 | 12,848 | (541,050) | (254,382) | (533,635) | 7,415 | (45,120) | (18,129) | (48,513) | (3,393) |
| Sports | 1,188,907 | 609,282 | 1,189,422 | 515 | (1,877,998) | (924,603) | (1,886,927) | (8,929) | (118,671) | (43,516) | (103,194) | 15,477 |
| Youthwork | 113,678 | 41,239 | 113,678 | 0 | (1,891,719) | (869,539) | (1,865,909) | 25,810 | (88,704) | (51,020) | (88,969) | (265) |
| Service Fee | 16,646,339 | 8,323,170 | 16,646,339 | 0 |  |  |  | 0 |  |  |  | 0 |
| HC Financial  Support | 2,764,000 | 0 | 2,764,000 | 0 | 0 |  |  |  |  |  |  | 0 |
| **Surplus/**  **(Deficit)** | **35,931,214** | **16,415,234** | **35,855,354** | **(75,860)** | **(30,084,047)** | **(14,586,913)** | **(30,118,703)** | **(34,656)** | **(5,847,167)** | **(3,130,070)** | **(5,983,215)** | **(136,048)** |

40

###### Commentary by Service APPENDIX D

|  |  |  |
| --- | --- | --- |
|  | **Variance (Year End)** | **Notes** |
| Adult | 17,126 | Projected savings in staffing costs due to vacancies. The Service will transfer to Highland Council on 1st December. |
| Archives | 24,462 | Positive projected variance to budget due to additional income from Nucleus Archive in conjunction with savings in operating costs. |
| Facilities | (215,028) | Projected overspend in staffing due to additional Area Manager post, High Life Development investment and salary regradings. |
| Libraries | 57 | On budget |
| Management | (91,236) | £140k overspend in Other Costs due to increase in Insurance Premium partly offfset by vacancy management savings in Business Support. |
| Museums & Galleries | (39,303) | Income at Highland Folk Museum and North Coast Visitor Centre projected to be £79k below budget mitigated by related savings in cost of sales. |
| Music Tuition | 7,880 | Small projected positive variance due to additional income and savings in Other Costs. |
| Rangers | 16,870 | Additional income from sale of sports equipment mitigating small projected overspend in operating costs. |
| Service Fee | 0 | On budget |
| HC Financial Support | 0 | On budget |
| Sports | 7,063 | Positive projected variance to budget due to savings in operating costs. |
| Youthwork | 25,545 | Projected savings in staffing costs due to vacancy management including Area Manager for South. The Service will transfer to Highland Council on 1st December. |

41

##### Internal Audit Final Report

##### APPENDIX E



High Life Highland Data Protection

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | **Priority** | **No.** | **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 |
| Major issues that managers need to address as a matter of urgency. | High | 0 |
| 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 |
| 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 | | | |

|  |  |  |
| --- | --- | --- |
| **Distribution:** | **Report Ref:** | HLH01/010 |
| Chief Executive, HLH | **Draft Date:** | 24/07/24 |
| Director of Corporate Performance, HLH Corporate Services | **Final Date:** | 30/09/24 |
| Head of Finance, HLH Chief Executive  Head of Digital & Technology, HLH Corporate Services ICT Officer, HLH Corporate Services |  |  |

42

Corporate Performance and Information Governance Manager, Highland Council Corporate Services

1. **Introduction**
   1. The audit reviewed High Life Highland’s (HLH) compliance with data protection legislation. This legislation requires personal data to be processed in a way that protects the identity of individuals.
   2. The audit reviewed HLH’s control environment governing data protection. This covered assessing policies and procedures, examining a sample of systems and records holding personal data, and looking at how customer and employee data rights are upheld, including how breaches of data protection legislation are handled.
   3. Data Protection was the responsibility of all HLH employees, but the ICT team had specific responsibility for overseeing data protection compliance. They were assisted in this capacity by a Data Protection Officer (DPO), the Highland Council’s Corporate Performance and Information Governance Manager.
2. **Main Findings**
   1. *There was an effective governance framework in place to ensure compliance with Data Protection Act (DPA) and UK General Data Protection Regulations (UK GDPR).*

This audit objective was partially achieved. There was a data protection policy. However, this was a very brief document so relied on supporting guidance. Neither the policy or guidance set out the governance structure, and roles and responsibilities for the Board Committees and DPO had not been defined. The Policy only referred to customers’ personal information rather than other parties such as employees or third party processors. Guidance included the main provisions outlined in legislation and the Information Commissioner’s (ICO) website; however, it did not explain how the 7 principles of data protection are to be applied in HLH activities.

There was a governance structure in place in that the DPO and the Finance and Audit Committee (and in turn the Board) are responsible for reviewing data protection matters, although not via a formal written remit. However, there was little evidence that this was routinely undertaken; recent minutes show little reference to data protection beyond limited reporting of data breaches, with no formal governance structure on reporting these. There used to be a Data Protection Working Group which was set up to review data protection procedures and compliance and provide information to senior management, but that has been inactive for 2 years. (See recommendation M1). The risk register did not include any reference to data protection. (See recommendation M2)

There was no comprehensive list of data sharing agreements. Data sharing agreements are not mandatory, but it is good practice and advisable to define responsibilities between HLH and partner organisations. There were some such agreements, but these were not held in a single location. (See action plan Recommendation M3)

HLH’s data protection guidance states that sites (e.g. leisure centres, museums etc) should be subject to data protection audits involving physical inspections of their adherence to policy and procedure. These had not been undertaken for some time. The nature of HLH operations involves data processing over numerous sites across a large geographic area and currently, assurance cannot be given that data is being managed at all sites as required. In particular, audits of CCTV data held had not taken place (as required by HLH CCTV procedures) so there was concern that this potentially higher risk data was not being reviewed. The reasons for these not taking place were disruption to operations due to the COVID pandemic and a Corporate Delivery Review which had proposed to move responsibility for data protection to another team. The latter was no longer taking place so there is scope to re-start the audits and visits (See action plan Recommendation M3).

1

43

There was a satisfactory process for dealing with data breaches. There were few of these (12 in the last 3 years). A sample of 3 of these showed they had been well documented using ICO templates. 1 was deemed serious enough to report to the ICO, this was done in the required timeframe. Which breaches and the level of detail provided reported to the Board has changed over time (See action Plan recommendation M1).

* 1. *Personal data was processed in accordance with the UK GDPR principles.*

This audit objective was partially achieved. There were privacy notices covering most of the customer and employee interactions with HLH, setting out how data would be processed and why the data was needed creating the basis for consent where required. There was no privacy notice for complaints although this was rectified during the audit.

A sample of 7 systems used to process customer or employee information was reviewed against the UK GDPR principles. Overall, the systems were compliant with the principles particularly lawfulness, purpose limitation and data minimisation. Consent was obtained or purpose was specified e.g. a contractual relationship, and as referred to above privacy notices covered how data would be used. Data held was necessary for the activity. For accuracy the majority of data was entered by customers or employees and in the main was basic contact details.

However, scope for further improvement was identified, specifically on the principles of storage limitation and integrity & security:

* + - Data being held longer than required indicating a lack of adherence to retention schedules.
    - The ability on 1 system for all staff users to change the personal details of other users, for example changing access permissions and deleting users which would allow some users unnecessary access and control over other users’ personal data.
    - Sharing personal data via email which was less secure than other methods and increasing the risk of a data breach.

1

* + - Holding data off the system unnecessarily for example paper copies of data entered into the system.
    - On 1 system a key field (date of birth) was optional which raised the risk of customers having access to inappropriate content.

Enquiries with a sample of 6 HLH sites confirmed that whilst mostly compliant, there were instances where data was held off the systems (e.g. in hard copy or on personal or shared drives) unnecessarily and for longer than required. (See Action Plan Recommendation M4)

Third party providers were used to process data on HLH’s behalf for example platforms used to take payments or collecting data via surveys. The list of those used was not up to date, not all of these were covered by a formal contract or agreement, and it was not clear to customers what data these providers collected or how it was used. Assurance had not been obtained from all providers on how data was stored or what systems testing providers had undertaken to ensure data security. UK GDPR stipulates that the data controller, in this case HLH, has a responsibility for the actions of its third party processors (See Action Plan M3).

The rights of data subjects were clearly outlined on the HLH website and there was a satisfactory process for handling Subject Access Requests. Few of these have been received (11 in the last 5 years), and a sample of 3 of these were found to have been processed in the required timeframe and to the expected level of detail.

* 1. *There were effective training and communication processes to maintain awareness of data protection principles amongst HLH staff.*

This audit objective was partially achieved. Data protection training consists of staff being informed of the latest version of the Data Protection Guidance. This was delivered by 2 methods:

1) staff briefing meetings, and 2) on the staff website whereby individual staff log on and were informed of the need to complete this training, with sustained reminders each time they logged onto the HLH staff website. The latter method was not mandatory and not all staff had access to the staff website.

44

Revised guidance was issued in June 2024. As of July 2024, 457 of 908 staff had not completed the training via the website, including a member of the senior management team. The previous version of guidance was issued in December 2023 and as of July 2024, 351 staff had not completed that phase of training, this number included staff who did not have an IT account. There was increased risk that staff were not aware of their responsibilities for data protection which could lead to a data breach (See Action Plan recommendation M5).

1. **Conclusion**
   1. There was good evidence that HLH had worked to comply with the key principles of data protection legislation with detailed guidance and procedures. However, there was scope to set out the governance arrangements clearly in a more detailed policy. Overall, there were systems in place to help ensure compliance with the data protection principles. But there was scope to improve the data protection control environment, notably improving information management. Re-starting the data protection audits of sites should assist with this.

2

45

1. **Action Plan**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Priority** | **Finding** | **Recommendation** | **Management Response** | **Implementation** | |
| **Responsible Officer** | **Target Date** |
| M1 | Medium | There is scope to improve the governance framework to ensure that Data Protection legislation is fully complied with:  The Data Protection Policy only referred to customer’s personal information rather than other parties such as employees or third party processors. Also, this did not set out roles and responsibilities for data protection. The guidance did not explain the 7 data protection principles and how they should be complied with by HLH staff and contractors.  There were few references to data protection at Committee meetings and there was no written remit for the Finance and Audit Committee specifying its remit regarding data protection.  The GDPR working group had not met for several years and its actions were not formally reported to HLH Committees. | Governance arrangements should be reviewed to make accountability clearer:  The policy should be updated to cover all parties whose personal data is processed and should define roles and responsibilities regarding data protection. Guidance should be updated to explain the data protection principles.  Management should consider formalising Finance and Audit Committee’s remits for data protection and including as a standing item to Committee agendas.  The data protection working group should be re-started with activities and actions reported to the Finance and Audit Committee and in turn the Board. | A revised policy will be taken to the next Data Protection working group meeting for approval.  The Finance and Audit Committee’s remit for data protection will be formalised and be included as a standing agenda item. Finance report to include outcomes of annual data protection audit.  Data breach trends to be reported at the Performance Board.  The first meeting of the Data Protection Working Group (DPWG) with revised Terms of Reference has been held. This will meet every 2 months. | Head of Digital & Technology, HLH  Head of  Governance and Scrutiny, HLH  Head Digital & Technology, HLH  ICT Officer, HLH | 25/10/24  11/11/24  and then Ongoing  Ongoing  Complete |

3

46

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Priority** | **Finding** | **Recommendation** | **Management Response** | **Implementation** | |
| **Responsible Officer** | **Target Date** |
|  |  | There was change over time in what data breaches and the level of detail being reported to the Board. | Management should develop a framework to enable consistent decisions on when breaches require to be reported to the Board and the level of detail required. | ICO reportable breaches are reported within Finance Report that goes to the Board. Data breach trends to be reported at the Performance Board.  The level of reporting will be formalised in our Data Protection Policy referred to above. | Head of Finance and Head of Digital & Technology, HLH | Ongoing |
| M2 | Medium | There was no reference to data protection on the risk register. | Management should assess whether data protection needs to be on the risk register. | Creation of “HLH20A” compliance entry to risk register  which will include Data Protection. | Head of Investment and Programme Management, HLH | Complete |
| M3 | Medium | Compliance with data protection best practice could be improved as follows:  Data protection audits outlined in the HLH Data Protection Guidance had not taken place for some time.  There was no single, comprehensive and up to date list of data sharing agreements.  There was lack of detail on how all third parties process data and insufficient assurance that these | In house data protection audits should re-start with a programme of site visits to be established.  A single comprehensive up to date register of data sharing agreements should be compiled.  The list of third party data processors should be updated to ensure it is comprehensive and | The current audit form is under review. A revised form will be presented to the DPWG at 25/10/24. Staff who will undertake audits will be identified and appropriate training provided. ICT expects the audits will then commence early 2025 and be conducted on an annual basis.  DPWG will identify all data sharing agreements and identify where they are required. A central agreements register will be created and populated and amended when required.  DPWG will review the list of third-party processors. The website now directs customers | ICT Officer, HLH/Head of Digital & Technology, HLH  ICT Officer, HLH/Head of Digital & Technology, HLH  ICT Officer, HLH | 31/12/24  (for remit and training to be completed so audits  can start 2025)  31/10/24  Complete |

4

47

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Priority** | **Finding** | **Recommendation** | **Management Response** | **Implementation** | |
| **Responsible Officer** | **Target Date** |
|  |  | providers adhere to and test their compliance with data protection legislation. | explains how data is processed. HLH should be able to show customers the contractual relationship it has with these providers and evidence that these providers can provide assurance that they have taken appropriate measures to comply with data protection legislation.  HLH management should consider the benefits of an information asset register and decide if one should be created. | of the relevant part of each third-party processors’ website; however, it should be noted that Data Protection processing is agreed and formed as part of the contract and is part of the ongoing contract monitoring.  The Information Asset Register is to be developed in a phased manner over the coming year. This will be defined by process  e.g. Finance, then linked to Privacy Notices. Built in tracking for asset owner when Joiner/Mover/Leaver will have  an impact. | ICT Officer, HLH/ Head of Digital & Technology, HLH Records Manager, HLH | 30/09/25 |
| M4 | Medium | There was scope for further improvement identified specifically on the principles of storage limitation and integrity & security:  Data being held longer than required indicating a lack of adherence to retention schedules.  The ability on 1 system for all staff users to change the personal details of other users. | Systems should be reviewed to ensure:  Data is archived and disposed of in line with retention schedules and only held for as long as necessary.  User access rights and permissions should be reviewed to ensure information is only accessible on a need to know  basis and in line with job roles. | An instruction will be issued to all relevant staff on the need to comply with Corporate Retention Schedules and also included in the monthly staff newsletter. Compliance checks will be included in the aforementioned data protection audits.  This cannot be amended on current system but migration to a new system is planned for 2025. The new system will | ICT Officer, HLH  /Head of Digital & Technology, HLH. Head of Marketing & Engagement, HLH  Head of Digital & Technology, HLH | 30/11/24  30/04/25 |

5

48

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Priority** | **Finding** | **Recommendation** | **Management Response** | **Implementation** | |
| **Responsible Officer** | **Target Date** |
|  |  | Sharing personal data via email which was less secure than other methods and increasing the risk of a data breach.  Holding data off the system unnecessarily for example paper copies of data entered into the system (accident and incident forms, recruitment details, customer records).  On the Library system a key field (date of birth) was optional which raised the risk of customers not being correctly classified by age and potentially having access to less restricted content. | Use of email to share personal data is minimised.  Staff should be instructed on what information can be permitted to be held out with systems and where this should be located.  Completion of the date of birth fields should be mandatory to ensure correct age classification and enable appropriate content restrictions to be applied. | prevent users from being able to edit another’s log in details.  The use of Mailchimp for mailing lists will be promoted.  This information will be added to the next version of the DP Guidance and also included as part of the annual audits.  We will review the date of birth field to ensure it is populated. Then speak to Civica to determine field format and which will be mandatory. This will also improve reporting functionality. | Head of Digital & Technology, HLH  Head of Digital & Technology, HLH  Head of Libraries and Senior Network Librarian with support from Head of Digital & Technology, HLH | Complete  31/03/25  then Ongoing  31/12/24 |
| M5 | Medium | A significant number of HLH staff have not completed the last 2 phases of data protection training delivered via the staff website. | Staff should be instructed to complete the data protection training and periodic monitoring of completion rates should be undertaken with appropriate follow up to staff who do not comply. Follow ups should be prioritised using a risk based approach targeting those staff who potentially pose the highest data protection risk first. | Various training routes are in place: Staff Induction, team meetings, User Required Actions (staff database) plus regular discussion at the Performance Board.  A review of training available will take place including iHASCO and Traineasy.  A review of which job roles are critical for data protection training will be undertaken with | ICT Officer, HLH ICT Officer, HLH | 31/10/24  31/12/24 |

6

49

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Priority** | **Finding** | **Recommendation** | **Management Response** | **Implementation** | |
| **Responsible Officer** | **Target Date** |
|  |  |  |  | training (every 2 years) recorded.  We will edit the Traineasy data course for HLH (i.e. duplicate and amend existing THC course). | Head of Digital & Technology, HLH | 31/03/25 |

7