

ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Executive
Date:	17th March 2014
Subject:	Information Governance Project
Portfolio Holder(s):	Councillor Alwyn Rowlands
Head of Service:	Head of Function (Council Business)/Monitoring Officer
Report Author: Tel: E-mail:	Chief Executive
Local Members:	Not applicable

A –Recommendation/s and reason/s
<ul style="list-style-type: none"> • No decision required - Report at the request of the Executive, on the 13th January 2014. • The Council is required to process personal data in compliance with the principles set out in the Data Protection Act 1998. <p>In September 2013 the Information Commissioner’s Office (ICO) conducted an audit of the Council’s information governance arrangements and highlighted failings in the way in which the Council handles data security and records management.</p> <p>A failure to properly safeguard personal data may lead to fines of up to £500,000 against a corporate body and fines of up to £50,000 against individuals.</p> <p>To respond to the ICO’s concerns, an Action Plan was agreed between the Council and the ICO, and is being overseen by the Council’s Information Governance Project Board, which is focusing on improving:</p> <ol style="list-style-type: none"> 1. Policies & Strategies 2. Communication, Training & Guidance 3. Records Management 4. Access to Buildings, Information and Third Parties 5. Governance (Ownership) / Reporting Procedures <p>The work currently being undertaken by the Project Board will affect how all Council Services operate, and is intended to deliver the range of changes</p>

needed to mitigate any financial penalties in the future and to ensure that the Council operates within ICO guidelines.

- The current status of the project appears at Appendix 1. Appendix 2 contains the Project's Risk Register.

B – What other options did you consider and why did you reject them and/or opt for this option?

Not applicable

C – Why is this a decision for the Executive?

There is no Executive decision required at this stage but a further report to the Executive is proposed on the 22nd April 2014 when a formal request will be made for additional funding from the Executive's contingency to address the short and medium term issues highlighted by the ICO in relation to the Council's arrangement for the closure, destruction and archiving of closed files. In due course the Head of Profession (HR) will submit a further bid to the Executive to fund staff training and development.

CH – Is this decision consistent with policy approved by the full Council?

Yes

D – Is this decision within the budget approved by the Council?

Not relevant at this stage.

DD – Who did you consult?		What did they say?
1	Chief Executive / Strategic Leadership Team (SLT) (mandatory)	The Chief Executive is the author of the Report and the SLT has been consulted
2	Finance / Section 151 (mandatory)	
3	Legal / Monitoring Officer (mandatory)	Is the SIRO and has advised the Chief Executive on this Report

4	Human Resources (HR)	} All represented on the Information Governance Project Board
5	Property	
6	Information Communication Technology (ICT)	
7	Scrutiny	Not consulted
8	Local Members	Not consulted
9	Any external bodies / other/s	Not relevant

E – Risks and any mitigation (if relevant)		
1	Economic	
2	Anti-poverty	
3	Crime and Disorder	
4	Environmental	
5	Equalities	
6	Outcome Agreements	
7	Other	The Project being reported is the mitigation of the risk

F - Appendices:
Appendix 1 Highlight Report
Appendix 2 Risk Register

FF - Background papers (please contact the author of the Report for any further information):
The ICO Report, Action Plan and agendas and minutes of the Project Board are available to all Members.

ATODIAD/APPENDIX

1

Project Highlight Report – 6th March 2014

Project Title:	Information Governance	Project Start Date:	1st November 2013
Project Lead: <i>(e.g. HoS/Manager)</i>	Lynn Ball	Project Expected End Date:	31st August 2014
Project Manager: <i>(include contact details):</i>	Laura James-Mowbray ljmed@anglesey.gov.uk	Reporting Period:	November 2013 - March 2014

RAG STATUS KEY:

Red – Definite problem identified and to be addressed;

Amber – Potential problems have been identified;

Green - This element of the programme/project is currently okay

1	Overall Status <i>[This is the mechanism that the Project Manager uses to show <u>their</u> assessment of how the project is progressing. This overall RAG status is supported by the comments of the Project Manager in 1.1 and the subsequent RAG status of each section]</i>	R
1.1	<p><i>Please insert a statement here from the Project Manager on the overall status of the project to support the RAG</i></p> <p>Of the 64 activities listed on the project plan in its entirety, 40 affect this period:</p> <p>Complete: 13 In progress: 12 Over running: 12 Awaiting CIO return: 3</p> <p>Currently based on the number of tasks overrunning their schedule (some at over 3 months), the overall assessment would place the project in RAG status – RED.</p> <p>There is however confidence in the ability to complete a large number of these tasks over the next 7-14 days. If not there is a danger that the activities those overrunning may be prerequisite to will slip. This will affect the project end date, project resources (and associated costs/budget) and finally the projects ability to deliver all activities as planned to the ICO.</p>	

2	On Budget <i>[Is the project delivering to budget? What is the percentage (%) and amount (£) of the variance?]</i>	G
2.2	The percentage over or under budget is: 0%	The amount over or under budget is: £0

3	On Time <i>[Is the project delivering on time? How many days/weeks is it ahead or behind schedule?]</i>	G
3.1	<p>The project is delivering to (+/-) 0 days/weeks</p> <p>Although the project has many activities that are over running, these activities currently do not affect the overall end date of the project. However if these activities continue to overrun and key resources (ICT and HR) are not recruited soon there is a likelihood that the project end date will be affected.</p> <p>This will need to be monitored closely and the status amended and reported upon if this becomes evident. It is however hoped that the project team can complete on the majority of the overrunning activities over the next 7-14 days removing any concerns.</p>	

4	Key Activity This Period <i>[Provide brief details of what has been achieved in the period since the last report. Use the RAG status to indicate if you have achieved the key activities you intended to achieve, as stated in the previous highlight report]</i>	R
	<p>Within this period a range of new or amended policies have been adopted these include:</p> <ul style="list-style-type: none"> ✓ Access to information policy ✓ Privacy Impact Assessment Policy ✓ Fair Processing Policy ✓ Personal Data Classification Policy ✓ Data Breach Policy ✓ Information Risk Policy <p>Other elements completed and reviewed as far as was necessary as part of the project include:</p> <ul style="list-style-type: none"> ✓ Home working Policy ✓ Processes for reviewing DPA within schools ✓ PIA template created for Project Documentation ✓ Corporate template (contract/agreement) for all data processor relationships ✓ Floor checks now being conducted at the end of the day ✓ CCTV signs reviewed, additional put up ✓ Appropriate SIRO training identified and arranged for late 2014 <p>Project Management:</p> <ul style="list-style-type: none"> ✓ A Project Manager has been appointed ✓ The Project Initiation Document is now in its LIVE format ✓ The Risk Register has been compiled and is being reviewed ✓ Work has commenced on the communications plan ✓ Message from the CEO released on Y Ddolen/Medra and available on MonITor <p>Although progress has been made, we are still without key members of staff (ICT and HR) which should have been recruited within this period. We also have a large number of activities which should have been completed within this period overrunning.</p>	

5	<p>Key Activity Next Period</p> <p>By the board meeting for the 8th May 2014, the project would hope to have achieved the following:</p> <ul style="list-style-type: none"> ▪ Appointment of both an ICT and a HR officer to the project ▪ A corporate template and process for logging removal of manual personal data ▪ A Standard fair processing notice template ▪ A corporate records retention schedule ▪ A roles and responsibilities document for the role of SIRO ▪ A definition of the role of <i>Information Asset Owners</i> including the designation of HoS to these roles ▪ Formal reporting lines for information risk ▪ A records management policy (and strategy) ▪ A revised Corporate DPA compliance policy ▪ An Information Security Policy ▪ An Information Asset Register ▪ All staff to be in receipt of the new ID/Swipe card combination ▪ A corporate Records Retention Schedule ▪ Updated web pages (MonITor) ▪ A corporate e-mail policy ▪ A central log of third party service contracts and agreements ▪ Record destruction collection points (lockable) made available across the authority ▪ A clear communication plan for the project
----------	---

6	Open or Major Risks/Issues				R
	<p><i>[Report the details of the risks and issues that are affecting the status of the project (e.g. directly responsible for the overall status being red or amber). This information should be taken from the Project Risk Register]</i></p>				
	Date Raised	Description	Risk/Issue Owner	Impact of Risk/Issue on Project	Planned Resolution
1.	January 2014	<p>Communications The risk that the project fails to communicate and engage effectively with key stakeholders</p>	HJ / SRO	<p>Key messages lost, Staff are not engaged, Project has no sustainability, Breaches to DP still being made, Failure to deliver agreed ICO action plan</p>	<p>Ensure staff up to date, Communication simple and frank, Maintain serious and urgent nature of messages, Provide training</p>
2.	January 2014	<p>Resource/ Capacity The risk of not being able to realize the project plan within the allocated time due to conflicting priorities and a lack of resources</p>	SRO	<p>Failure to deliver agreed ICO action plan, Posts remaining vacant, Increase in key staff sickness levels, Risk of financial penalties, Negative media</p>	<p>Urgently recruit both ICT and HR posts, Options appraisal for the resourcing of cleansing the Council's storage facility.</p>

3.	January 2014	Resource/ Budget The risk that an insufficient review of need and cost will lead to problems in terms of scope as the project progresses	SRO	Negative/Detrimental effect on project scope in terms of quality and/or timescale Breaches to DP being made Risk of financial penalties Negative media	Work to be undertaken on the work packages required for larger project related tasks, Pre-empt the resources and budget required, Secure required resources ahead of task commencement
4.	January 2014	Ownership/ Buy-in The risk that without ownership from services the project will not be able to deliver successfully in terms of culture change	SLT	Project will be unable to progress at the rate required, Staff will not be fully engaged, Key messages lost, Project has no sustainability, Breaches in DP still being made, Failure to deliver to agreed ICO action plan	High level communication with all service heads and principal officers, Ensure buy-in to the project and its planned deliverables, Monitoring of data processes via IoACC Audit Plan

Project Lead Name:	Lynn Ball	Date:		Additional Comments:	
HoS Name (if different from Lead)	N/A	Date:	N/A	Additional Comments:	N/A

Information Governance Project

Status Update 06.03.2014

ljimed@anglesey.gov.uk

COMPLETE	
Action Ref.	Action Description
1.2	Review and amend the <i>Access to Information Policy</i>
1.4	Create a <i>Privacy Impact Assessment Policy</i>
1.6	Produce a Corporate <i>Fair Processing Policy</i>
1.7	Produce a Corporate <i>Personal Data Classification Policy</i>
1.8	Produce a <i>Data Breach Policy</i>
1.11	Produce an <i>Information Risk Policy</i>
2.5	Identify and secure appropriate SIRO training
3.8	Review the potential for ensuring any service hardware databases directly feed into and are consistent with corporate hardware database
4.1	A review of the prominence of and adequacy of CCTV notices in connection with Council offices
4.2	Ensure Principal Building Surveyors team conducts floor checks at end of day
4.12	Develop a corporate template for future use in connection with all data processor relationships
5.9	Review existing regulatory activity and append to this action plan any outstanding actions
5.12	Prepare a PIA template to be included in corporate 'Project Documentation'

MAKING PROGRESS AND WITHIN TIMESCALE	
Action Ref.	Action Description
1.1	Revise Corporate <i>DPA Compliance Policy</i>
1.3	Prepare an <i>Information Security Policy</i> for both electronic and manual records
2.1	Creation of DPA 'How to' flow charts
2.2	Design and go live with corporate IG web pages
2.3	Corporately branded IG campaign using posters where appropriate
3.2	Undertake an audit across the authority to establish the authority's information assets and reflect the findings in the corporate Risk Register. Produce an Information Asset Register to be maintained by the CIO
3.4/3.6	Implement the findings of the review of the general storage arrangements for manual records and personal data held at alternative council buildings
3.5	Obtaining appropriate assurances from our suppliers of confidential waste destruction
4.3	Introduce standard photo ID's (combined with swipe card) to all staff throughout the authority
4.4	Review access to the main foyer with the intention of preventing visitors from accessing the main building without authorisation
4.5	Check existing employees have appropriate levels of swipe card access and that cards of former employees have been disabled.
4.14	An audit of third party service contracts and agreements for each service to be undertaken to develop and maintain a central log.

OVERRUNNING TARGET END DATE

Action Ref.	Action Description	Owner	End date	Update	Mitigation
3.1	Corporate records retention schedule will be developed and adopted	CIO/ICT Manager	13.01.14	Retention policies requested from all HoS, GCC have shared theirs	Responses to be received and evaluated
3.3	A corporate template and process will be developed for logging the removal of manual personal data from its usual location	CIO	15.11.14	Form drafted	Process complete once discussions with ICO have taken place
3.7	Property service to identify suitable locations within service areas as record destruction collection points	Property Manager	13.12.13	Discussions with providers on-going	
4.6	Review password controls for casework systems for greater uniformity of length, complexity and expiry. Reflect findings in Information Security Policy	ICT Manager	22.11.13	Work undertaken, 10 systems identified, multitude of passwords need to be entered before reaching any system. Decision taken that current arrangements are sufficiently robust	Now need to re-word the information security policy to reflect this decision then the action will be complete
4.8	Define, review and provide a report on 'shared' accounts to be included within the Information Security Policy	ICT Manager	06.12.13	A list of shared accounts identified, any idle for 30+ days has been disabled (42 accounts disabled). Some accounts must remain 'shared' these are for customer service reasons – these will however have no internet or e-mail access i.e. library/cashier desks	Now need to re-word the Information security policy to reflect this, then the action will be complete

4.9	Undertake a review that considers printers/faxes: 1) Being turned off outside business hours 2) Scanned items to be sent to a network device and NOT saved on the scanner/printer memory Reflect findings in the information security policy	ICT Manager	17.01.14	Work ongoing regarding purchasing/destroying MFD internal hard-disks upon end of lease period. (Suppliers contacted to discuss options)	
4.11	Ensure precautions are in place and communicated: ‘Files not to be saved locally/externally or printed when accessing corporate server remotely’	ICT Manager	28.02.14	Access to these functions can be universally blocked via webmail. Could not prevent print screen or e-mailing to personal e-mail. This could only be achieved by removing web mail and providing only officers that need remote access with the tools to do so... laptops/tablets/smartphone	ICT currently investigating the practicalities of this requirement
4.13	Write a contract and issue to current courier in order to formalise the data controller/processor relationship	Passed from CIO to Property	15.11.13 (passed on 03.03.14)	The data processing agreement has been written and sent.	As the authorising of invoices is done by property, the contract needs to be written by them.
4.15	Develop a standard fair processing notice (FPN) template, and undertake a review of existing FPN's to update and amend before transferring to corporate template	CIO	31.01.14	FPN's received from services, drafted and approved by project board 06/03/2014	This item is now ready to complete
5.3	Prepare a roles and responsibilities document for the role of SIRO	CIO	24.01.14	Roles documents sources and to be reviewed	This item is near completion

5.5	Develop a process to show the formal reporting lines for information risk	CIO	07.02.14		Allocated to interim agency worker
5.6	Define the role of the IAO and designate service heads. This will be reflected in the risk management strategy and the process for reporting information risks	CIO to be passed to HR	31.01.14	Paper drafted.	Agreement needed to progress via HR

ATODIAD/APPENDIX 2

Risk Register

Notes:

- (i) Each individual risk has been designated a 'Responsible Officer', who will be responsible for progressing the mitigating action(s) and providing updates to the *Project Manager*.
- (ii) 'Risk' will be an agenda item at each meeting of the *Project Board*, and reflected on the *Highlight Report*

Risk Reference	Risk Owner / Lead Officer	Date Identified or Amended	Risk Identified		Risk Level			Additional Control Measures / Treatment Required			Residual Risk Level			Review Date / Frequency
			Vulnerability / Hazard	Consequences / What or who will be effected and how / Outcome / Effect on objectives	Likelihood	Severity	Score	Action	Responsible Officer	Score	Review Date	Likelihood	Severity	
1.	HJ/SRO	Jan 2014	COMMUNICATIONS The risk that the project fails to communicate and engage effectively with key stakeholders	<ul style="list-style-type: none"> ▪ Staff are not engaged ▪ Key messages are lost ▪ Requests to change processes are going ignored ▪ Project deliverables has no sustainability ▪ Breaches in DP still being made ▪ Risk of further advisories ▪ Risk of financial penalties ▪ Negative media attention ▪ Failure to deliver on agreed ICO action plan 	4	4	16	<ul style="list-style-type: none"> ▪ Keep communication simple and frank ▪ Keep all staff updated on developments in the simplest and shortest format ▪ Maintaining the serious and urgent nature of the message ▪ Training provided to all current staff ▪ Training included in induction of all new staff ▪ Supported by a poster/communications campaign to act as reminders to staff 	GJ/CE & PM					
2.	SRO	Jan	RESOURCES /		4	4	16	<ul style="list-style-type: none"> ▪ The PM has now been appointed 20/01/14 	CE & BE					

Risk Reference	Risk Owner / Lead Officer	Date Identified or Amended	Risk Identified		Risk Level			Additional Control Measures / Treatment Required			Residual Risk Level			Review Date / Frequency
			Vulnerability / Hazard	Consequences / What or who will be effected and how / Outcome / Effect on objectives	Likelihood	Severity	Score	Action	Responsible Officer	Score	Review Date	Likelihood	Severity	
		2014	CAPACITY The risk of not being able to realise the project plan within the allocated time due to conflicting priorities and a lack of resources	<ul style="list-style-type: none"> ▪ Failure to deliver on agreed ICO action plan ▪ Posts remaining vacant for some time pushing back progress on the agreed action plan ▪ Noted increase in key staff sickness levels ▪ Slow progress being made on both IG project and day to day work, this risks not only failure to deliver the ICO action plan but also to deliver business as usual on local priorities ▪ Negative media attention ▪ Risk of financial penalties 				<ul style="list-style-type: none"> ▪ Urgently recruit for the post of HR & ICT ▪ Options appraisal for the resourcing of the work package 'cleansing hen Ysgol y Graig' Secondment/recruitment of resources to hen ysgol y graig 						
3.	SRO	Jan 2014	RESOURCES / BUDGET The risk that an insufficient review of need and cost will lead to problems in terms of scope as the project progresses	<ul style="list-style-type: none"> ▪ Negative/detrimental effect on project scope in terms of quality expected by the ICO ▪ Negative/detrimental effect on project scope in terms of timescale agreed with the ICO ▪ Or both ▪ Breaches in DP still being made ▪ Risk of further advisories ▪ Risk of financial penalties ▪ Negative media attention ▪ Failure to deliver agreed ICO action plan 	4	4	16	<ul style="list-style-type: none"> ▪ Work to be undertaken on the work packages required for the larger tasks that sit within the scope of this project ▪ Pre-empt the resources and budget needed ▪ Secure such resources ahead of task commencement due date 	DE & PM					
4.	SLT	Jan 2014	OWNERSHIP / BUY-IN	<ul style="list-style-type: none"> ▪ Project will be unable to progress at the rate required ▪ Staff will not be fully engaged without the direction and buy-in of their services ▪ Key messages will be lost ▪ Requests to change 	4	4	16	<ul style="list-style-type: none"> ▪ High level communication with all service heads and principal officers ▪ Ensure buy-in to the project and its planned deliverables through full understanding of urgency/ importance and risks 	SRO					

Risk Reference	Risk Owner / Lead Officer	Date Identified or Amended	Risk Identified		Risk Level			Additional Control Measures / Treatment Required			Residual Risk Level			Review Date / Frequency	
			Vulnerability / Hazard	Consequences / What or who will be effected and how / Outcome / Effect on objectives	Likelihood	Severity	Score	Action	Responsible Officer	Score	Review Date	Likelihood	Severity		Score
			The risk that without ownership from services the project will not be able to deliver successfully in terms of culture change.	<ul style="list-style-type: none"> processes will be ignored ▪ Project deliverables have no sustainability ▪ Breaches in DP still being made ▪ Risks of further advisories ▪ Risk of financial penalties ▪ Negative media attention ▪ Failure to deliver agreed ICO action plan 				<ul style="list-style-type: none"> associated with not achieving the planned changes. ▪ Monitoring of protective marking and Data Processes via the IoACC Audit Plan 							

Likelihood:

1 = Rare

2 = Unlikely

3 = Possible / Moderate

4 = Likely

5 = Almost Certain / Already happening

Severity:

1 = Insignificant

2 = Minor

3 = Moderate

4 = Major

5 = Catastrophic

Score = Likelihood x Severity