Information Governance Audit

1. Summary Findings

Organisation:	Overall Opinion	Good Assurance	Previous outcome	Adequate Assurance	Direction of Travel	Higher compliance
Chelmsford County High School for Girls	Audit Sponsor:	Melissa Mulgrew			Report Issued	10/07/2019

Summary Findings

Congratulations on your improving compliance, you have shown commitment to complying with the new legislation. You now need to build on your positive start and use the recommendations from your recent audit to further improve.
You need to have a documented role description for the SIRO.
Please publish the Data Protection Statutory Policy with the overarching Privacy Notice on your website.
Once completed your security measures document can also be published to provide assurance that you have appropriate measures in place to secure personal data.
Please consider your email retention policy to help you manage technical security and achieve data minimisation.

Audit Areas Overview:

Roles	Policy	Reporting	Notification	Assets

Flows	Training	Retention	Risk	Suppliers

Requests	Incidents	Assessment	Notices	Consent

Biometrics	Photo/Video	CCTV	Marketing	Security

Colour Key

	Critical priority issues identified
	Major priority issues identified
	Moderate priority issues identified
	No / Minor Issues identified
	Not assessed as part of this audit by request or not applicable

igs | Essex County Council

1. Audit areas

Previous	statement	Findings	New
A. General			
	1) Your published documentation makes reference to your DPO.	In Place	
	2) You have a documented role description for the SIRO.	Not in Place (No progress)	
	3) There is a current ICO registration at the correct tier.	In Place	
	4) Additional security is applied to Biometric data.	In Place	
	5) There are effective processes in place to ensure that the use of personal data for surveys and marketing purposes (other than directly for the school) is done in compliance with privacy law, including the Privacy of Electronic Communications Regulations (PECR)	N/A	

	6) Staff recognise complaints and requests under Data Protection rights and direct the request to an individual responsible for co-ordinating with the DPO.	In Place	
Comments			
B. Reporting			
	7) You are completing your B1 reporting tool.	In Place	
	8) You regularly provide reporting analysis data to your SLT and/or Governors.	In Place	
Comments			
C. Policy			
	9) All of the framework policies are in place.	In Place	
	10) The Data Protection and Statutory request policies are published on your website.	Partially in Place (In progress)	
	11) Policies have been circulated to staff.	In Place	
	12) Policies have been reviewed and ratified by SLT/Governors.	In Place	
Comments			
D. Procedures			
	13) Procedures in the framework have been adopted.	In Place	
	14) Policies are reviewed annually and changes are recorded in your policy change log.	In Place	
	15) You have adopted and published the Framework privacy notices on your website.	In Place	
	16) Your data collection forms/letters point to your online privacy policy.	In Place	
	17) You have published the data protection policy statement with your privacy notices.	Partially in Place (In progress)	
	18) Consent is only sought when it is genuinely required.	In Place	
	19) You have a written process for recording and managing the refusal or withdrawal of consent.	In Place	

	20) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage	In Place	
	21) The personal data you collect for your purposes is actively minimised.	In Place	
	22) (*Where necessary*) An impact assessment is carried out on your surveillance equipment	In Place	
	23) (*Where necessary*) Surveillance footage can be accessed to respond to a request for information.	Partially in Place (In progress)	
	24) (*Where necessary*) Adequate surveillance signage is in place.	In Place	
	25) A culture of reporting security incidents is embedded in the school.	In Place	
	26) Staff are trained to recognise security incidents and manage them appropriately.	In Place	
	27) Security incident data is regularly analysed to capture lessons learned.	In Place	
	28) Student/Staff records have been cleansed to meet the retention timeframe.	Partially in Place (In progress)	
	29) Electronic storage, including emails, is managed in line with the retention policy.	Partially in Place (In progress)	
	30) Data is structured in a way that supports effective management of retention.	Partially in Place (In progress)	
	31) Staff complete GDPR eLearning annually.	In Place	
	32) There is a method for recording training for staff/volunteers/governors.	In Place	
	33) Formal training is supported by communications or briefings.	In Place	
	34) All new staff receive data protection induction training.	In Place	

Comments

E. Sharing Data with Partners & Suppliers

	35) All new contracts include the contract schedule template and the 3rd party policy requirements.	In Place	
	36) The Information Sharing Protocol with ECC has been signed up to on the Essex Schools Infolink,	In Place	
	37) All volunteers/work experience students have signed a non-disclosure agreement.	N/A	
	38) All suppliers have been contacted and GDPR assurances received.	In Place	
	39) A process is in place to handle requests for personal data for the prevention or detection of crime or fraud.	In Place	

Comments			

F. Statutory Requests for Information			
	40) All requests for information are logged on your B1 reporting tool.	In Place	
	41) All statutory requests are handled in line with the framework procedure.	In Place	
	42) Your website carries a publication scheme for Freedom of Information requests.	In Place	

Comments			

G. Risk Management			
	43) The risk register is reviewed and updated annually.	In Place	
	44) Data Protection Impact Assessments (DPIAs) have been completed for high risk processing.	In Place	
	45) Employees with the authority to buy software or engage suppliers are aware of the need to consult the individual who conducts Data Protection Impact Assessments	Partially in Place (In progress)	

Comments			

H. RoPA			
	46) The Information Asset Register is completed and reviewed annually.	In Place	
	47) The Data Flows have been mapped and reviewed annually.	In Place	
	48) The security measures documented has been completed and is reviewed/updated annually.	Partially in Place (In progress)	

Comments			

3. Action Plan

The following areas have been identified as requiring action in order to improve compliance. The Audit Area column below contains the reference to the Audit Area above for which an appropriate control is not in place. Please use the 3 columns below on the right (headings in grey) to track your progress in resolving this.

Audit Area	Actions Required	Name of Task Owner	Target Date	Completion Date
General				
2	The Headteacher would typically undertake the SIRO role. Ensure the IGS role template (Ref:A1) is combined with an existing role description for the SIRO role-holder. The role holder must be made aware of the requirements of their SIRO duties.			
Reporting				
Policy				
10	Follow the guidance in Document D11 (Publishing for Transparency) in order to ensure that the key policies are available to parents/ guardians on your school website. Ensure both the Data Protection and Statutory Request policies are published on your website.			
Procedures				
17	Publish the Data Protection Policy Statement at Annex E of the Privacy Notice Procedure (D2). This statement should be published alongside your online privacy notices to ensure compliance with the law			
23	(Where necessary) Ensure any surveillance equipment has the capability to download any data to respond to a request for information. Ensure that, if necessary, data can be removed from any downloads to protect third party information (Ref.D5)			
28	You must carry out a review of digital and paper pupil records, securely deleting/destroying those outside of the retention period (unless you have a justifiable reason to keep them which has been documented).(Ref.D8)			

29	1) Adopt policy and develop documented processes for systems so that staff are clear on where and how to document their activities to support easy searching for data and to reduce duplication. Consider adopting and amending the IGS Records Management Policy (Ref:C8). 2) Consider removing 'personal' storage areas to improve the school's overview of where its data is held - or otherwise confirm that administrator rights exist to search for data across all systems. 3) Consider re-organising shared document storage areas into clear subject structures which are well maintained and where access to sensitive data is controlled.			
30	Review information held within archive / storage areas and destroy information that is no longer required or is past the recommended retention period. Ensure information within storage is clearly labelled with destruction dates to make this easier in future			
Sharing Data with Partners & Suppliers				
Statutory Requests for Information				
Risk Management				
45	Assign responsibility for an employee within the school to be the point of contact for managing assessments. Ensure this employee knows to engage the DPO over assessments at the earliest stage in order to gain expert advice			
RoPA				
48	The Security Measures document should accurately reflect your Organisational and Technical Security (Ref:H2). The organisational section should be agreed with any key stakeholders who manage aspects of the measures referred to in the document. Your IT support should confirm whether the technical aspects are an accurate representation of how technology is currently managed to keep personal data secure. This should follow a consideration of the risks posed by the current provision and reflect any agreed changes as a result of a risk review			

4. Basis of our Opinion and Assurance Statement

Level	Overall Assurance Rating Description
Good	***Good assurance*** – there is a sound system of internal control designed to achieve the objectives of the system/process and manage the risks to achieving those objectives. Recommendations will normally only be of Low risk rating. Any Moderate recommendations would need to be mitigated by significant strengths elsewhere.
Adequate	***Adequate assurance*** – whilst there is basically a sound system of control, there are some areas of weakness, which may put the system/process objectives at risk. There are Moderate recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any Major recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.
Limited	***Limited assurance*** – there are significant weaknesses in key areas in the systems of control, which put the system/process objectives at risk. There are Major recommendations or a number of moderate recommendations indicating significant failings. Any Critical recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.
No	***No assurance*** – internal controls are generally weak leaving the system/process open to significant error or abuse or reputational damage. There are Critical recommendations indicating major failings

Auditors' Responsibilities: It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses. However, Audit procedures alone, even when carried out with due professional care, do not guarantee that non-compliance will be detected. Accordingly, our examinations as auditors should not be relied upon solely to disclose non–compliant practices, unless we are requested to carry out a special investigation for such activities in a particular area.

Auditor:	Orla O'Shea	**Distribution List:**	**Releasing Audit Reports:** Draft and final reports are retained by Essex County Council for 6 years and only distributed outside the Council's Information Governance Team to the named individuals on the distribution list above. Approval for distributing this report wider should be sought from the relevant Audit sponsor. Care must be taken to protect the control issues identified in this report.
Fieldwork Completed:	10/07/2019	Melissa Mulgrew	
Final Report:	10/07/2019		

Risk Rating	Audit Area Assessment Rationale
 **Critical**	Major financial loss – Large increase on project budget/cost: (Greater of **£1.0M** of the total Budget or more than **15 to 30%** of the organisational budget). Statutory intervention triggered. Impacts the whole Organisation. Cessation of core activities. Strategies not consistent with government's agenda, trends show service is degraded. Failure of major projects – Senior Managers/ Governing bodies are required to intervene. Intense political and media scrutiny i.e. front-page headlines, TV. Possible criminal, or high profile, civil action against the organisation and its employees. Life threatening or multiple serious injuries or prolonged work place stress. Severe impact on morale & service performance. Strike actions etc.
 **Major**	High financial loss – Significant increase on project budget/cost: (Greater of **£0.5M** of the total Budget or more than **6 to 15%** of the organisational budget). Service budgets exceeded. Significant disruption of core activities. Key targets missed, some services compromised. Management action required to overcome medium term difficulties. Scrutiny required by external agencies, Audit Commission etc. Unfavourable external media coverage. Noticeable impact on public opinion. Serious injuries or stressful experience requiring medical treatment, many workdays lost. Major impact on morale & performance of more than 50 staff.
Moderate	Medium financial loss – Small increase on project budget/cost: (Greater of **£0.3M** of the total Budget or more than **3 to 6%** of the organisational budget). Handled within the team. Significant short-term disruption of non-core activities. Standing Orders occasionally not complied with, or services do not fully meet needs. Service action will be required. Scrutiny required by internal board to prevent escalation. Probable limited unfavourable media coverage. Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale & performance of up to 50 staff.
 **Minor**	Minimal financial loss – Minimal effect on project budget/cost: (**< 3%** Negligible effect on total Budget or **<1%** of organisational budget) Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule. Handled within normal day to day routines. Internal review, unlikely to have impact on the corporate image. Minor injuries or stress with no workdays lost or minimal medical treatment. No impact on staff morale.