IGS - Information Governance Audit

1. Summary Findings

Organisation:	Overall Opinion	Good Assurance	Previous outcome	Good Assurance	Direction of Travel	Static Compliance
Chelmsford County High School for Girls	Audit Sponsor	Melissa Muldrew	Previous audit date	10/07/2019	Date of this Audit	22/06/2020

Summary Findings	Audit Areas Overview:			Colour Key	
Congratulations on maintaining your compliance, you have shown commitment to complying with the legislation. You now need to build on your positive start and use the recommendations from your audit to further improve. Ensure you have non-disclosure agreements in place for school volunteers, and keep focussed on transparency ensuring all your privacy notices and policies are published on your website. Continue to fully utilise your reporting tool and ensure that you complete data privacy impact assessments where needed, seeking support from IGS as and when you need it. Well done on a successful year, keep up this direction of travel.	Roles	Policy	Reporting		Critical priority issues identified
	Records	Risk & Security	Training		Major priority issues identified
	RoPA	Sharing	Suppliers		Moderate priority issues identified
	Transparency	Marketing	Surveillance		No / Minor Issues identified
					Not assessed as part of this audit by request or not applicable
				wnewton@cchs.essex.sch.uk	

2. Audit areas

Statement	Findings	New
A. Roles & Responsibilities		
1) Your published documentation makes reference to your DPO.	In Place	
2) You have a documented role description for the SIRO and the role is assigned.	In Place	
3) There is a current ICO registration at the correct tier, and a process in place to renew annually by an identified role.	In Place	
Comments		
B. Policy & Procedure		
4) All of the framework policies are in place.	In Place	
5) Policies have been reviewed and ratified by SLT/Governors.	In Place	

6) Policies are reviewed annually and changes are recorded in your policy change log.	In Place	
7) You have documented evidence that annually or at induction staff read, understand and agree to abide by your policies.	In Place	
8) Procedures in the framework have been adopted.	In Place	
Comments		
C. Reporting		
9) Your B1 Reporting Tool is fully utilised and regularly reviewed.	In Place	
10) Insight from reporting data is used to inform training and awareness activities and for policy/procedure reviews	In Place	
11) You regularly provide reporting analysis data to your SLT and/or Governors.	In Place	
Comments		
D. Records Management		
12) The personal data you collect for your purposes is actively minimised.	In Place	
13) Student/Staff records have been cleansed to meet the retention timeframe.	Partially in Place (in progress)	
14) Electronic storage, including emails, is managed in line with the retention policy.	Partially in Place (in progress)	
15) Data is structured in a way that supports effective management of retention.	In Place	
Comments		
E. Risk & Security		
16) The security measures document has been completed and is reviewed/updated annually.	Partially in Place (in progress)	
17) A culture of reporting security incidents is embedded in the school.	In Place	

18) Staff are trained to recognise security incidents and manage them appropriately.	In Place	
19) Security incident data is regularly analysed to capture lessons learned and shared with staff to raise awareness.	In Place	
20) The risk register is reviewed and updated annually.	In Place	
21) Data Protection Impact Assessments (DPIAs) have been completed for high risk processing and recorded on your B1 reporting tool.	Partially in Place (in progress)	
22) Employees who buy software or engage suppliers are aware of the need to consult the individual who conducts Data Protection Impact Assessments	In Place	
23) Your school network and broadband connection are penetration tested annually and the results recorded on your B1 reporting tool	In Place	
24) Security Patches are applied promptly and recorded on your B1 reporting tool	In Place	
25) Business Continuity plans are in place and regularly tested	In Place	
26) Disaster Recovery Plans are in place to bring systems back up in the event of a major incident	In Place	
Comments		
F. Training & Awareness		
27) Staff complete GDPR eLearning annually and within one month of joining the organisation. Training and awareness activities are logged on your B1 reporting tool	In Place	
28) Training is delivered to volunteers and Governors, and recorded.	Partially in Place (in progress)	
29) Formal training is supported by communications or briefings.	In Place	
30) All new staff receive data protection induction training within one month of joining the organisation.	In Place	
Comments		
G. Records of Processing Activities (RoPA)		
31) The Information Asset Register is completed and reviewed annually.	In Place	
32) The Data Flows have been mapped and reviewed annually.	In Place	

33)Overseas transfers are identified and appropriate safeguards recorded.	In Place	
Comments		
H. Sharing Data		
34) The Information Sharing Protocol with ECC has been signed up to on the Essex Schools Infolink	In Place	
35) Information Sharing Agreements are put in place for regular data sharing which is not supported by a contract and is not a statutory return required by law.	In Place	
36) Non-disclosure agreements are signed where appropriate.	Partially in Place (in progress)	
Comments		
I. Suppliers		
37) All new contracts include the contract schedule template and the 3rd party policy requirements.	In Place	
38) All suppliers have been contacted and GDPR assurances received.	In Place	
39) New suppliers complete the Supplier Security Questionnaire.	In Place	
Comments		
J. Transparency		
40) You have adopted and published the Framework privacy notices on your website and these are reviewed annually, or earlier when there are changes to technology or data is processed in a new way.	In Place	
41) Your data collection forms/letters point to your online privacy policy.	In Place	
42) You have published the data protection policy statement with your privacy notices.	Partially in Place (in progress)	
43) The documents in the Publishing for Transparency procedure have been uploaded to your website.	Partially in Place (in progress)	
44) Consent is only sought when it is genuinely required.	In Place	

45) You have a written process for recording and managing the refusal or withdrawal of consent.	Partially in Place (in progress)	
46) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage	In Place	
47) All requests for information are logged on your B1 reporting tool.	In Place	
48) All statutory requests are handled in line with the framework procedure.	In Place	
49) Your website carries a publication scheme for Freedom of Information requests.	In Place	
50) Staff recognise complaints/requests under Data Protection rights and direct them to an individual responsible for co-ordinating with the DPO.	In Place	
51) A process is in place to handle requests for personal data for the prevention or detection of crime or fraud and clear records are kept.	In Place	
52) Additional security is applied to Biometric data and your Privacy Notice is available on your website. Additionally a policy on the use of Biometrics must be in place.	Partially in Place (in progress)	
Comments		
K. Marketing		
53) There are effective processes in place to ensure that the use of personal data for surveys and marketing purposes is done in compliance with privacy law, including the Privacy of Electronic Communications Regulations (PECR)	In Place	
Comments		
H. Surveillance		
54) An impact assessment is carried out on your surveillance equipment (this includes CCTV, Body Worn Cameras, Drones, Automated Number Plate Recognisiton, and any other surveillance mechanism)	In Place	
55) Surveillance footage/soundbites can be accessed to respond to a request for information.	In Place	
56) Adequate surveillance signage is in place.	In Place	
57) Privacy Notices make clear that surveillance is in operation and advises the legal basis and how to exercise data subject rights	In Place	
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	Target Date	Complete Date
Roles & Responsibilities				
Policy & Procedures				
Reporting				
Records Management				
13	You must carry out a review of digital pupil and staff records, (eg those held on SIMs / Integris) securely deleting those outside of the retention period (unless you have a justifiable reason to keep them which has been documented).(Ref.D8)			
14	Ensure data held in emails and network drives is not kept longer than is necessary by agreeing a retention policy for emails. Inform staff that they must regularly remove emails that are not required. Data such as emails or reports should be stored in a central area, such as with the pupil file, and then deleted from personal systems. This will assist you in future when requests are made for someone's personal data, and to ensure that the personal information is deleted when it should be.			
Risk & Security				
16	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.			
21	Data Protection Impact Assessments (DPIAs) must be completed for all new systems that will collect personal information. The DPO should sign off any DPIAs for systems involving high risk processing (eg high volumes of data; special category data). All DPIAs must be logged on your B1 reporting tool.			
Training & Awareness				
28	Use your B1 reporting tool to record training for staff/volunteers/governors.			
RoPA				
Sharing Data				
36	Ensure NDAs are completed where appropriate (Ref:E6) and are retained in line with records of directly employed staff in order to ensure that complaints received about the individual after they left can be supported for a reasonable period by evidence of the school's controls.			
Suppliers				
Transparency				

42	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			
43	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. Ensure the Rights for Parents notice is on your website.			
45	A documented process must be in place for managing consents and ensure that it is as easy to withdraw consent as to give it. Careful records must be maintained to ensure that if someone has refused or withdrawn consent for an activity, that their data is not used for that purpose going forward (Ref.D3)			
52	Additional security must be applied to Biometric data and you must have a privacy notice online to cover the use of such data; and a policy must be in place (Refs.C3&D2)			

Marketing

Surveillance

4. Basis of our Opinion and Assurance Statement

Level	Overall Assurance Rating Description
Good Assurance	***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 Assurance	***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 Assurance	***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 Assurance	***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.

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.