IGS - Information Governance Audit

1. Summary Findings

Organisation:	Overall Opinion	Adequate Assurance	Previous outcome	Limited Assurance	Direction of Travel	Higher Compliance
Shenfield High School	Audit Sponsor	Stuart Roberts	Previous audit date	06/01/2021	Date of this Audit	15/11/2021
	Audit Conducted By:		Lucie Walker			

Summary Findings	Audit Areas Overview:			Colour Key	
The compliance score has improved to adequate assurance which is to be applauded. However, there are still some key areas which require work. The website needs some attention as some policies are incomplete, out of date or duplicated. This should be a simple task but one which ensures transparency. Updating the RoPA will also allow the school to locate and manage risks. Supplier risk also needs to be managed. This can be done with robust contracts (E1), DPIAs and making sure you are aware where the school's data is being processed. Steps have already been taken to improve records management which is great. Please keep up this direction of travel and contact IGS for support when necessary.	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
				Email address of Chair of Governors for Governor Report: j.swettenham@shenfield.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		
SIRO role is carried out bu Stuart, Finance Manager. This is under review.		
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.	Partially in Place (in progress)	
8) Procedures in the framework have been adopted.	In Place	
Comments		
Staff are sent policies for consultation before they are approved by governors.		
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 which is presented and discussed at a full Governors meeting at least annually.	Partially in Place (in progress)	
Comments		
Data protection is duscussed annually following an audit. This is to become a more regular occourance.		
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.	In Place	
14) Electronic storage, including emails, is managed in line with the retention policy.	Not in Place (in progress)	
15) Data is structured in a way that supports effective management of retention for example files names should carry a date of creation to aid management of retention	Not in Place (in progress)	
Comments		
E. Risk & Security		
16) The security measures document has been completed and is reviewed/updated annually.	In Place	

17) A culture of reporting security incidents is embedded in the school.	Partially in Place (in progress)	
18) Staff are trained to recognise security incidents and manage them appropriately.	Partially in Place (in progress)	
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 processing involving personal data (including systems) and recorded on your B1 reporting tool.	In Place	
22) When completing DPIAs where it involves a data processor you explore whether the contractor uses sub-contractors in delivering the service and in which country they are based.	In Place	
23) Employees who 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)	
24) Your school network and broadband connection are penetration tested annually and the results recorded on your B1 reporting tool	Partially in Place (in progress)	
25) Security Patches are applied promptly and recorded on your B1 reporting tool	Partially in Place (in progress)	
26) Business Continuity plans are in place and regularly tested	In Place	
27) Disaster Recovery Plans are in place to bring systems back up in the event of a major incident	In Place	
Comments		
Message to be sent to team leaders to remind them about software. Pen testing has been completed but not recorded. A culture of reporting security incidents needs to be embeded within the school.		
F. Training & Awareness		
28) Staff complete GDPR Training annually and within one month of joining the organisation. Training and awareness activities are logged on your B1 reporting tool	In Place	
29) Training is delivered to volunteers and Governors, and recorded.	In Place	
30) Formal training is supported by communications or briefings.	Not in Place (no progress)	
31) All new staff receive data protection induction training within one month of joining the organisation.	In Place	
Comments		
IGS newsletters will be forwareded to all staff		

G. Records of Processing Activities (RoPA)		
32) The Information Asset Register is completed and reviewed annually.	Partially in Place (in progress)	
33) The Data Flows have been mapped and reviewed annually.	Partially in Place (in progress)	
34) Overseas transfers are identified and appropriate safeguards recorded and reflected in contracts/agreements	Not in Place (in progress)	
Comments		
RoPA on school's template. Being moved to the IGS one.		
H. Sharing Data		
35) The Information Sharing Protocol with ECC has been signed up to on the Essex Schools Infolink. If your Local Education Authority is not Essex, please ensure your local authority has a data sharing agreement in place which you have signed for the sharing between you. This is recorded on your B1	Partially in Place (in progress)	
36) 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. For example with Community Health Providers for heath services and system updates. All ISPs are referenced in your RoPA and on your B1.	In Place	
37) Non-disclosure agreements are signed where appropriate.	Not in Place (in progress)	
Comments		
No volunteers in 2 years. Will make them sign an NDA in the future		
I. Suppliers		
38) Contracts are in place for all suppliers where personal data is stored or processed.	In Place	
39) Suppliers outside the UK who are storing/processing personal data have appropriate safeguards, for example approved standard contract clauses in place in the contract/agreement between you. This is recorded on RoPA.	Partially in Place (in progress)	
Comments		
J. Transparency		
40) You have adopted and published the latest version of 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) The documents in the Publishing for Transparency procedure D11 have been uploaded to your website.	In Place	

42) Your data collection forms/letters point to your online privacy policy.	In Place	
43) Consent is only sought when it is genuinely required.	In Place	
44) You have a written process for recording and managing the refusal or withdrawal of consent.	Not in Place (no progress)	
45) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage.	Not in Place (no progress)	
46) All requests for information are logged on your B1 reporting tool.	In Place	
47) All statutory requests are handled in line with the framework procedure.	In Place	
48) Your website carries a publication scheme for Freedom of Information requests.	In Place	
49) Staff recognise complaints/requests under Data Protection rights and direct them to an individual responsible for co-ordinating with the DPO.	In Place	
50) 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.	Not in Place (no progress)	
51) 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.	In Place	
Comments		

K. Marketing		
52) 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)	Not in Place (no progress)	
Comments		
Will add PTA activity to the website instead of the newsletter.		
H. Surveillance		
53) An impact assessment is carried out on your surveillance equipment (this includes CCTV, Body Worn Cameras, Drones, Automated Number Plate Recognition, and any other surveillance mechanism)	In Place	
54) Surveillance footage/soundbites can be accessed to respond to a request for information.	In Place	
55) Adequate surveillance signage is in place.	Not in Place (no progress)	

56) Privacy Notices make clear that surveillance is in operation and advises the legal basis and how to exercise data subject rights	In Place	

Comments

Signage for CCTV needs to be installed.

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	Complete Date
Roles & Responsibilities				
Policy & Procedures				
7	The school should make policies available to all staff who handle personal data. This can be on a school intranet, network drive, emailed directly to staff or provided as hard-copy. Use the Policy Change Log (D1) to record when the policy was disseminated. Reference to policies should be made during inductions for new staff and through any refresher training. You should document annually staff commitment to read, understand and abide by the policies.			
Reporting				
11	Regular reporting analysis should be provided to your SLT and/or Governors to enable them get a clear picture of the school's compliance with Data Protection and provide comment on the data and set actions as a result. Lessons learned should be shared with staff in order to raise awareness and protect against further similar incidents. Policy reviews must take account of any breach analysis to ensure policies remain fit for purpose.			
Records Management				
14	Ensure data held in emails and network drives is not kept longer than is necessary. Agree a retention policy for emails and inform staff that they must regularly remove emails that are not required. Emails that do need to be kept should be stored in a central area, such as with the pupil file, and then deleted from email system. With network files, staff should be made aware that any data (for example school reports/assessments etc) they hold for pupils that have left the school, should be deleted from the network, or anonymised. 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.			
15	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			
Risk & Security				
17	Staff must be trained, and regularly reminded, how to recognise a security incident and how to report it. (Ref.D10)			
18	Use the Security Incident Management procedure (Document D6) to assist with defining the school's process for handling security incidents. All incidents must be logged on your B1 and incident outcome forms must be completed. Staff must be aware of the action to be taken if a Security Incident occurs.			
23	Assign responsibility for an employee within the school to be the point of contact for managing DPIAs. Ensure this employee knows to engage the DPO over assessments at the earliest stage in order to gain expert advice			

24	Penetration testing must be carried out at least annually and the results recorded on your B1 reporting tool to ensure your network is not vulnerable to cyber attacks			
25	Security Patches must be applied at the earliest opportunity and recorded on your B1 reporting tool. The application of security patches is necessary to prevent data loss, corruption or theft.			
Training & Awareness				
30	Formal training should be supported by communications or briefings which enable you to share lessons learned and support understanding. Communications, briefings and formal training should all be recorded on your B1 reporting tool			
RoPA				
32	Review the content on the information asset register (Ref:H1 - IAR Tab) making sure all required information is entered so that the entries are 'complete'. Ensure entries for all systems you use are included on the register.			
33	Complete the list of Data Flows to ensure that all the data that flows in and out of the assets identified on the IAR tab of your ROPA is recorded. Begin with pupil and staff records (paper and digital); SEN records and Safeguarding/Child Protection files as your priority, then address any remaining assets.			
34	You must identify and log any flows where data transfers outside of the UK and ensure that you have documented the safeguard you are relying on. If in doubt seek advice from IGS.			
Sharing Data				
35	Review and sign up to the Education sharing agreement on the ESI to support the sharing of data between your school and the local authority. It can be found on the Essex Schools Infolink in The Data and Standards/Information Governance/Information Sharing Protocol between schools and colleges page. If your LEA is not Essex you must consider what data you routinely share with your LEA and make sure that this is supported by an agreement. All ISPs must be recorded on B1			
37	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				
39	Where Processors or sub-processors are based outside the UK you must have in place an appropriate safeguard. You can find out locations by checking the suppliers website or contacting them directly.			
Transparency				
44	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)			
45	Consent for photo/video must be split into the different uses the school may wish to use it for e.g. displays; use on website; use on social media. Use and retention should be clearly stated in privacy notices. (Ref.D2)			
50	Ensure staff are aware of how to handle requests for personal data for the prevention or detection of crime or fraud. Ensure all requests are logged and documented (Ref E8)			
Marketing				

52	Privacy statement and notices should identify and explain marketing activity and how a recipient can request discontinuation. Manage requests to withdraw consent for marketing on appropriate systems which are monitored. (Ref.D2)			
Surveillance				
55	Clearly visible and adequate signage must be in place to meet your legal obligation. It must state surveillance is in operation, along with: The name of the Data Controller (School name); The name of the Data Protection Officer; The purpose of the processing; Data Subjects rights; How to access the full privacy notice (web address) (Ref.D5)			

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.