IGS - Information Governance Audit

1. Summary Findings

Organisation:	Overall Opinion	Limited Assurance	Previous outcome	Adequate Assurance	Direction of Travel	Lower Compliance
Shenfield High School	Audit Sponsor	Stuart Roberts	Previous audit date	15/10/2019	Date of this Audit	06/01/2021

Summary Findings

It has been a difficult year but there is still much work to do to position your school where it can adequately defend itself if challenged over its data protection practices. Compliance with the law requires organisations to provide documented evidence of how they manage personal data. You currently have limited evidence in place and this needs to be rectified.
You demonstrated a general awareness of the need for information security, but this is not documented through your policies and procedures. Please ensure that you log security incidents. The logging of incidents is paramount in understanding the risks faced by the school, and evidencing your intent to manage such incidents properly.
Please ensure that the mandatory GDPR training is completed by all staff and logged on your reporting tool. Please remember IGS are there to support you with advice and guidance should you need it.

Audit Areas Overview:

Roles	Policy	Reporting
Records	Risk & Security	Training
RoPA	Sharing	Suppliers
Transparency	Marketing	Surveillance

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

j.swettenham@shenfield.essex.sch.uk

2. Audit areas

Statement	Findings	New
A. Roles & Responsibilities		
1) Your published documentation makes reference to your DPO.	Partially in Place (no progress)	
2) You have a documented role description for the SIRO and the role is assigned.	Partially in Place (in progress)	
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.	Partially in Place (no progress)	
5) Policies have been reviewed and ratified by SLT/Governors.	Partially in Place (in progress)	

6) Policies are reviewed annually and changes are recorded in your policy change log.	Partially in Place (in progress)	
7) You have documented evidence that annually or at induction staff read, understand and agree to abide by your policies.	Not in Place (in progress)	
8) Procedures in the framework have been adopted.	Not in Place (in progress)	
Comments		
C. Reporting		
9) Your B1 Reporting Tool is fully utilised and regularly reviewed.	Partially in Place (no progress)	
10) Insight from reporting data is used to inform training and awareness activities and for policy/procedure reviews	Not in Place (in progress)	
11) You regularly provide reporting analysis data to your SLT and/or Governors.	Not in Place (in progress)	
Comments		
D. Records Management		
12) The personal data you collect for your purposes is actively minimised.	Partially in Place (in progress)	
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.	Partially in Place (in progress)	
15) Data is structured in a way that supports effective management of retention.	Partially in Place (in progress)	
Comments		
E. Risk & Security		
16) The security measures document has been completed and is reviewed/updated annually.	Not in Place (no progress)	
17) A culture of reporting security incidents is embedded in the school.	Not in Place (in progress)	

18) Staff are trained to recognise security incidents and manage them appropriately.	Not in Place (in progress)	
19) Security incident data is regularly analysed to capture lessons learned and shared with staff to raise awareness.	Not in Place (in progress)	
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.	Not 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	Partially in Place (in progress)	
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	Not in Place (no progress)	
28) Training is delivered to volunteers and Governors, and recorded.	Not in Place (no progress)	
29) Formal training is supported by communications or briefings.	Not in Place (in progress)	
30) All new staff receive data protection induction training within one month of joining the organisation.	Not in Place (no progress)	
Comments		
G. Records of Processing Activities (RoPA)		
31) The Information Asset Register is completed and reviewed annually.	Partially in Place (in progress)	
32) The Data Flows have been mapped and reviewed annually.	Partially in Place (in progress)	

33)Overseas transfers are identified and appropriate safeguards recorded.	Not in Place (no progress)	
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.	Partially in Place (in progress)	
36) Non-disclosure agreements are signed where appropriate.	In Place	
Comments		
I. Suppliers		
37) All new contracts include the contract schedule template and the 3rd party policy requirements.	Partially in Place (in progress)	
38) All suppliers have been contacted and GDPR assurances received.	Partially in Place (no progress)	
39) New suppliers complete the Supplier Security Questionnaire.	Partially in Place (in progress)	
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.	Not in Place (no progress)	
41) Your data collection forms/letters point to your online privacy policy.	Partially in Place (in progress)	
42) You have published the data protection policy statement with your privacy notices.	Not in Place (no progress)	
43) The documents in the Publishing for Transparency procedure have been uploaded to your website.	Not in Place (no 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	Partially in Place (in progress)	
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.	Not in Place (no progress)	
50) Staff recognise complaints/requests under Data Protection rights and direct them to an individual responsible for co-ordinating with the DPO.	Partially in Place (no progress)	
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.	Not 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)	Partially in Place (in progress)	
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)	Not in Place (no progress)	
55) Surveillance footage/soundbites can be accessed to respond to a request for information.	In Place	
56) Adequate surveillance signage is in place.	Partially in Place (in progress)	
57) Privacy Notices make clear that surveillance is in operation and advises the legal basis and how to exercise data subject rights	Not in Place (no 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	Target Date	Complete Date
Roles & Responsibilities				
1	Ensure your published documentation, such as your privacy notices, make reference to your DPO (Ref.D2)			
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.			
Policy & Procedures				
4	Ensure you have a complete set of Information Governance policies in place. Use the IGS policies provided in Section C of the Framework if you cannot demonstrate that these are covered by existing policies. If you intend to adopt the IGS policies without amendment, ensure that they are reviewed before adopting and publishing so that the school is confident that it has the processes in place to fulfil the commitments made. If you wish to amend policies so that they accurately reflect the explicit rules the school wishes staff to follow, ensure decisions are risk assessed and documented.			
5	There must be a documented process to ratify school policies, with policies reviewed annually and any changes noted in the policy change log (D1)			
6	A clear timetable must be in place which shows which policies are due for review and that there is a clear process for reviewing current polices, suggesting amendments based on information about their current effectiveness as well as any lesson learned from security incidents and submitting them to the approving body and publishing. Use the policy change log (document D1) to capture details of policy reviews and maintaining an accurate record over time of what has changed and when			
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.			
8	Procedures must be in place and made available to relevant staff to ensure the appropriate handling of personal data			
Reporting				
9	Use the reporting template (document B1) to record relevant data (eg FOI/EIR, SAR, Security Incidents, Training, IT, Surveillance, RoPA, Records Management) in order to evidence the school's compliance with the Accountability principle required in law.			
10	The insight from the analysis of your reporting tool content must be used when developing or refreshing training material and when reviewing policies and procedures to ensure all are fit for purpose and manage risks effectively.			
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				
12	Only collect the relevant personal data that is necessary for the activity (Ref.D4)			

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.			
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				
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.			
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.			
19	Use analysis information from your security incidents to inform any updates to policy, training or technical controls which may be necessary.			
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.			
22	Ensure that all staff are aware that DPIAs must be completed prior to purchasing new systems that will collect or process personal information, and that they know who to consult, within the school, in order to manage this process. Ensure you engage the DPO over assessments at the earliest stage in order to gain expert advice.			
Training & Awareness				
27	Staff must complete the GDPR eLearning module annually and this must be recorded on your B1 reporting tool.			
28	Ensure governors complete refresher training annually; the virtual training provided by IGS can be used for this. This should be added to your B1 reporting tool to record training.			
29	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			
30	A checklist for induction activities should be reviewed to ensure it contains details of all relevant policies, procedures and guidance resources, and completed checklists are signed and filed appropriately as a record of completion. Use document D10 for guidance			
RoPA				
31	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.			
32	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.			

33	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	Data sharing must be supported by a contract, Memorandum of Understanding or Information Sharing Protocol. These must be in place to evidence your compliance with data protection principles. In some circumstances it will be those requesting data from you that will need to provide you with an appropriate document to support its sharing, e.g. NHS			
Suppliers				
37	All new contracts must include the contract schedule template and the 3rd party policy requirements as this provides evidence of your compliance with GDPR (Refs.E1&E2)			
38	GDPR assurances provided by suppliers must be appended to their record.			
39	All new suppliers of systems/software have completed the Supplier Security Questionnaire			
Transparency				
40	Review the template privacy notices (Annex C of document Ref:D2) and determine which are relevant to the processing undertaken in the school and publish them on your website alongside your overarching privacy notice. Review them annually for accuracies or whenever there are changes to technology or data is processed in a new/different way			
41	The forms you use (paper or digital) to obtain personal data (e.g. Admissions form) must direct the data subjects to the relevant privacy notice(s) which explain the processing.(Use the statement found on document Ref:D2, Appendix D)			
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)			
46	Consent for photo/video must be split into the different uses the school may wish to use it for eg displays; use on website; use on social media. Use and retention should be clearly stated in privacy notices. (Ref.D2)			
49	Ensure your website carries a publication scheme for Freedom of Information requests in line with statutory requirements (Ref.F4)			
50	Employees must be made aware of GDPR rights to a level where a request made under the rights is recognisable, and they are able to direct the request to an individual within the school responsible for co-ordinating with the DPO. This should also include recognition of FOI and EIR requests and should be achieved through standard training and awareness activities (document D10)			
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				
53	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				
54	All surveillance equipment must be risk assessed and those assessments are regularly reviewed and recorded (Ref.D5)			
56	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)			
56	The 'Managing Security' privacy notice is displayed on the school website, supported by the overarching privacy notice. Where necessary the school has updated the Managing Security notice with additional surveillance methods, e.g. ANPR, BWC etc (other than CCTV).			

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.