IGS - Information Governance Audit

1. Summary Findings

Organisation:	Overall Opinion	Adequate Assurance	Previous outcome	Adequate Assurance	Direction of Travel	Static Compliance
Shenfield High School	School Audit Attendees	Stuart Roberts	Previous audit date	15/11/2021	Date of this Audit	30/01/2023
	Audit Conducted By:		Orla O'Shea			
DP Lead:	Stuart Roberts		SIRO:		Claire Costello	

Summary Findings

Congratulations on your compliance, you have shown commitment to complying with the legislation. It is concerning that so few security breaches have been recorded in this academic year, as this is likely to indicate that either you are not aware of breaches when they occur, or there is poor understanding of what a security breach is. I recommend that you instil a culture of reporting security incidents and ensure that all staff understand what an incident is, and what they need to do. We strongly recommend all staff complete the GDPR Basics training to further their understanding. Keep focussed on transparency ensuring all your privacy notices and policies are published on your website. 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.

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

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.	Partially in Place (in progress)	
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.	Not in Place (in progress)	

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.	Not 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.	Partially 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	Partially in Place (in progress)	
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		
D. Records Management		
12) The personal data you collect for your purposes is actively minimised. Only necessary information is collected for each processing activity.	Partially in Place (no progress)	
13) Student/Staff records have been cleansed to meet the retention timeframe.This includes all systems which hold student or staff records, not just your main Information Management System.	In Place	
14) Electronic storage, including emails, is managed in line with the retention policy.	In Place	
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	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.	Partially in Place (in progress)	
18) Staff are trained to recognise security and cyber 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.	Partially 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 processing involving personal data (including systems) and recorded on your B1 reporting tool.	Partially in Place (in progress)	
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.	Partially in Place (in progress)	
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	In Place	
25) Security Patches are applied promptly and recorded on your B1 reporting tool	In Place	
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		
F. Training & Awareness		
28) Staff complete GDPR Training annually. Training and awareness activities are logged on your B1 reporting tool	Partially in Place (in progress)	
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		
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	Partially in Place (in progress)	
Comments		
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.	Not in Place (in progress)	
37) Non-disclosure agreements are signed where appropriate.	N/A	
Comments		
I. Suppliers		
38) A GDPR compliant contract is in place for all suppliers where personal data is stored or processed.	Partially in Place (in progress)	
39) The contract must reflect the relationship between the school and supplier. E.g. Data Controller to Data Processor or Data Controller to Data Controller.	Partially in Place (in progress)	
40) Where you have signed up to a supplier's Terms and Conditions you have checked whether all content from your own contract schedule are covered. If they are not, you have supplemented with your own contract schedule (E1 / E2) and advised the supplier that an assumption has been made that they can fully comply with your schedule unless they contact you to discuss.	Partially in Place (in progress)	
41) 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		
42) 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.	Partially in Place (in progress)	
43) The documents in the Publishing for Transparency procedure D11 have been uploaded to your website.	Partially in Place (no progress)	

44) Your data collection forms/letters point to your online privacy policy.	Partially in Place (in progress)	
45) Consent is only sought when it is genuinely required.	In Place	
46) You have a written process for recording and managing the refusal or withdrawal of consent.	Partially in Place (no progress)	
47) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage.	Partially in Place (in progress)	
48) All requests for information are logged on your B1 reporting tool.	In Place	
49) All statutory requests are handled in line with the framework procedure.	In Place	
50) Your website carries a publication scheme for Freedom of Information requests.	Not in Place (no progress)	
51) Staff recognise complaints/requests under Data Protection rights and direct them to an individual responsible for co-ordinating with the DPO.	In Place	
52) 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	
53) 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 (no progress)	
Comments		

K. Marketing

54) 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). Be aware, marketing is not just supplying goods and services for renumeration, it includes the promotion of ideals and aims.	In Place	
Comments		

H. Surveillance

55) 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	
56) Surveillance footage/soundbites can be accessed to respond to a request for information; either directly from school managed systems or by contractual arrangements if your system is supplied by a 3rd party provider.	In Place	
57) Adequate surveillance signage is in place.	Partially in Place (in progress)	
58) Privacy Notices make clear that surveillance is in operation and advises the legal basis and how to exercise data subject rights	In Place	

59) All requests to access surveillance data either directly from the school (internally) or a supplier or 3rd party are logged.	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 Owner	Target Date	Complete Date
Roles & Responsibilities				
1	Ensure your published documentation, such as your privacy notices, make reference to your DPO (Ref.D2)			
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.			
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. Ensure staff sign to confirm they have read the following policies: Data Protection (C3); Acceptable Personal Use (C5); Data Security Handling (C6)			
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 (e.g. 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)			
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. In additon you should display cyber security awareness materials to ensure staff are aware of risks and how to report, defend against and/or mitigate any attacks.			
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 (e.g. high volumes of data; special category data). All DPIAs must be logged on your B1 reporting tool, and added to RoPA.			
22	Establish in which country sub-contractors are based by reviewing their websites or contacting them directly. If you use an international cloud infrastructure (e.g. Amazon Web Services, Microsoft 365, Google Cloud) assess if your data will be transferred outside the UK. Wherever possible request that your data is stored in the UK. All processing outside the UK must be recorded on your H1 RoPA along with any safeguards relied on for that processing.			
23	Assign responsibility for an employee within the school to be the point of contact for managing DPIAs. Ensure all staff know to consult this employee prior to engaging new suppliers or downloading any new systems or software where personal data will be used. Ensure this employee knows to engage the DPO over assessments at the earliest stage in order to gain expert advice			
Training & Awareness				
28	Staff must complete GDPR training annually, either by scheduled sessions for staff to watch IGS GDPR Basics video, or attending an IGS presented session, or accessing/attending other Data Protection training. This must be recorded on your B1 reporting tool.			
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. There should be at least 1 flow for every asset, though some assets (such as pupil and staff records (paper and digital); SEN records and Safeguarding/Child Protection files) will require multiple flows. Use the examples provided in the IGS RoPA template (Ref:H1), then address any remaining flows.			
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			
36	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. You must record on RoPA which data flows are supported by either a contract, an information sharing protocol or memorandum of understanding, and note this on your B1.			
Suppliers				
38	You must ensure that new contractors complete either the relevant contract schedule (E1/E2) or, if they have provided you with a contract / Terms and Conditions to sign up to, that you have checked them to ensure they contain all content that is included in your own contract schedule			
39	The contract must reflect the relationship between the school and supplier. You should use E1 for Data Contoller to Data Processor and E2 for Data Controller to Data Controller. This ensures the correct responsibilities have been assigned to the data.			
40	If you have signed up to a supplier's Ts and Cs you must check whether all content from your own contract schedules (E1 & E2) are covered. If they are not you must supplement with your either E1 or E2 and advise the supplier that an assumption has been made that they can fully comply with your schedule unless they contact you to discuss further.			
41	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				
42	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			
43	Follow the guidance in Document D11 (Publishing for Transparency) in order to ensure that the key documents are available to parents/ guardians on your school website. This includes guidance documents for parents, Rights for Parents and Parents Guide to Subject Access Requests.			
44	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)			
46	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)			
47	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 your website carries a publication scheme for Freedom of Information requests in line with statutory requirements (Ref.F4)			
53	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				
57	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.	