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	School Audit Attendees	Melissa Mulgrew	Previous audit date	06/05/2022	Date of this Audit	25/04/2023
	Audit Conducted By:		Oliver Sharpe			
DP Lead:	Melissa Mulgrew		SIRO:		Stephen Lawlor	

Summary Findings	Audit Areas Overview:			Colour Key	
The school have worked hard to ensure their compliance, which has resulted in them retaining a good assurance outcome. They have demonstrated several areas of good practice such as a complete B1 reporting tool; completion of DPIAs for all systems used; and a complete Records of Processing Activity (RoPA). The school only have a couple of actions following on from this audit, one of which is to ensure that Governor's complete GDPR training. Another action is that consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage. The positive outcome and the school's commitment are to be commended.	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	
				wnewton@cchs.co.uk	

2. Audit areas

Statement	Findings	New
A. Roles & Responsibilities		
1) You have published the most recent framework documentation which 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/Trustees.	In Place	
6) Policies are reviewed annually taking into account any statutory changes, data breaches which occurred in the past year, and any feedback from staff. These 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		
C. Reporting		
9) Your B1 Reporting Tool is fully utilised, **including the technology tab,** and regularly reviewed.	In Place	
10) Insight from reporting data is used to inform training and awareness activities and policy/procedure reviews	In Place	
11) You regularly provide reporting analysis data to your SLT and Governors/Trustees which is presented and discussed at a full Governors/Trustees meeting at least annually.	In Place	
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.	In Place	
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 and regularly deleted. Paper records are managed in line with retention and regularly weeded and considered for secure destruction.	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.	In Place	
17) A culture of reporting data breaches is embedded in the school.	In Place	
18) Staff are trained to recognise data breaches and cyber incidents and manage them appropriately.	In Place	
19) Security breach 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 you must determine which country the supplier is based in; and if outside the UK ensure an appropriate safeguard is in place and recorded on your RoPA.	In Place	
23) Employees who buy software or engage suppliers are aware of the need to consult the individual who conducts DPIAs	In Place	
24) Your school network and broadband connection are penetration tested annually and the results recorded on your B1 reporting tool	In Place	
25) Security updates are routinely and regularly applied and recorded on your B1 reporting tool	In Place	
26) Business Continuity plans are in place and regularly reviewed and tested	In Place	
27) Disaster Recovery Plans are in place to bring systems back up in the event of a major incident and regularly reviewed	In Place	
Comments		
F. Training & Awareness		
28) Staff complete Data Protection (DP) training annually and this is logged on your B1 reporting tool	In Place	
29) DP Training is delivered to volunteers and Governors/Trustees, and recorded on your B1 reporting tool	Partially in Place (in progress)	
30) Ancilliary staff who do not have regular access to technology are provided with the DP Handout and this should be logged on your B1 reporting tool	In Place	
31) All new staff receive data protection induction training within one month of joining the school.	In Place	

32) Training is supported by DP awareness activities and communications which are logged on your B1 reporting tool	In Place	
Comments		
G. Records of Processing Activities (RoPA)		
33) The Information Asset Register is completed and reviewed annually.	In Place	
34) The Data Flows have been mapped and reviewed annually.	In Place	
35) Overseas transfers are identified and appropriate safeguards recorded and reflected in contracts/agreements	In Place	
Comments		
H. Sharing Data		
36) 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	In Place	
37) 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	
38) Non-disclosure agreements are signed where appropriate.	In Place	
39) Staff are aware that any requests to share data from police or other investigators (s212) are logged and handled in line with the data sharing procedure	In Place	
40) Where data is shared for safeguarding purposes, this is only done by the DSL or their representative, and is recorded on the relevant record.	In Place	
Comments		
I. Suppliers		
41) A data protection contract schedule is in place for all suppliers where personal data is stored or processed. If you sign up to a suppliers T&Cs you must ensure the schedule covers all elements of the E1/E2. If not, you must ask them to sign up to the E1/E2.	In Place	
42) The correct data protection contract schedule is in place according to the relationships involved, e.g. either E1 Controller to Processor or E2 Controller to Controller.	In Place	

43) Suppliers outside the UK who are storing/processing personal data have appropriate safeguards, for example an adequacy decision is in place and this is recorded on RoPA.	In Place	
44) If you use suppliers outside the UK in a country without an adequacy decision, you must complete a transfer risk assessment prior to entering into the contract and use an appropriate safeguard e.g., International Data Transfer Agreement (IDTA).	In Place	
Comments		
J. Transparency		
45) 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	
46) The documents in the Publishing for Transparency procedure D11 have been uploaded to your website.	In Place	
47) Your data collection forms/letters point to your online privacy policy.	In Place	
48) Consent is only sought when it is genuinely required.	In Place	
49) You have a written process for recording and managing the refusal or withdrawal of consent.	In Place	
50) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage.	Partially in Place (in progress)	
51) All requests for information are logged on your B1 reporting tool.	In Place	
52) All statutory requests are handled in line with the framework procedure.	In Place	
53) Your website carries a publication scheme for Freedom of Information requests.	In Place	
54) Staff recognise complaints/requests under Data Protection rights and direct them to an individual responsible for co-ordinating with the DPO.	In Place	
55) A process is in place to handle requests for personal data for the prevention or detection of crime or fraud (s212) and clear records are kept.	In Place	
56) 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		

57) 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.	N/A	
Comments		
H. Surveillance		
58) An impact assessment is carried out annually on your surveillance equipment (this includes CCTV, Video Doorbells, Body Worn Cameras, Drones, Automated Number Plate Recognition, and any other surveillance mechanism)	In Place	
59) 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	
60) Adequate surveillance signage is in place and Privacy Notices make clear that surveillance is in operation and advises the legal basis and how to exercise data subject rights	In Place	
61) 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
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. Ensure staff sign to confirm they have read the following policies: Data Protection (C3); Acceptable Personal Use (C5); Data Security Handling (C6)			
Training & Awareness				
29	Ensure training is delivered to Governors/Trustees and volunteers. This should be recorded on your B1 form			
Transparency				

50	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)			

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.