# 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 | 06/05/2021 | Date of this Audit | 06/05/2022 |
| | Audit Conducted By: | | Paula Girling | | SIRO: | Stephen Lawlor |
| DP Lead: | Melissa Mulgrew | | Secondary Contact: | | | |

**Summary Findings**

Congratulations on your compliance, you have shown commitment to complying with the legislation. You will need to ensure that there are adequate safeguards and a contract in place, but we will walk you through the process. As a priority, please ensure that the assets and data flows include all systems used and show whether they are held outside of the UK. Please work through the audit recommendations and remember to contact IGS for advice when you use a new supplier which handles personal data. Continue to fully utilise your reporting tool and ensure that you complete 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.

**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: wnewton@cchs.co.uk
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** | | |
| **1.** Please amend the email address of the DPO on the Main Overarching and the Alumae Privacy Notice to igs@essex.gov.uk | | |
| **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 which is presented and discussed at a full Governors 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. | 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. | In Place | |
| 18) Staff are trained to recognise security and cyber 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 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 | 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 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 | In Place | |
| 29) Training is delivered to volunteers and Governors, and recorded. | In Place | |
| 30) Formal training is supported by communications or briefings. | In Place | |
| 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. | In Place | |
| 33) The Data Flows have been mapped and reviewed annually. | In Place | |
| 34) Overseas transfers are identified and appropriate safeguards recorded and reflected in contracts/agreements | Partially in Place (in progress) | |
| **Comments** | | |
| **34.** Please remember to book a RoPA review after the summer holidays | | |
| **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 | In Place | |
| 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. | In Place | |
| **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 Processor. | In Place | |
| 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. | In Place | |
| **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. | In Place | |
| 43) The documents in the Publishing for Transparency procedure D11 have been uploaded to your website. | In Place | |
| 44) Your data collection forms/letters point to your online privacy policy. | In Place | |
| 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. | In Place | |
| 47) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage. | In Place | |
| 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. | In Place | |
| 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. | In Place | |
| **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. | N/A | |
| **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. | In Place | |
| 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 |
|---|---|---|---|---|
| **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. | | | |
| **RoPA** | | | | |
| 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. | | | |
| **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 | | | |
| 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. | | | |

## 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.