Chichester College Group

Data protection audit report

May 2023

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Chichester College Group (CCG) requested an audit from the ICO in November 2021, however the ICO was unable to accommodate an audit at this time. In January 2023 the ICO contacted CCG and a consensual audit of their data protection practices was agreed.

The purpose of the audit is to provide the Information Commissioner and CCG with an independent assurance of the extent to which CCG, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of CCG processing of personal data. The scope may take into account any data protection issues or risks which are specific to CCG, identified from ICO intelligence or CCG's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each

scope area to take into account the organisational structure of CCG, the nature and extent of CCG's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to CCG.

It was agreed that the audit would focus on the following area(s)

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
Training and Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, remote interviews with selected staff, and a virtual review of evidential documentation.

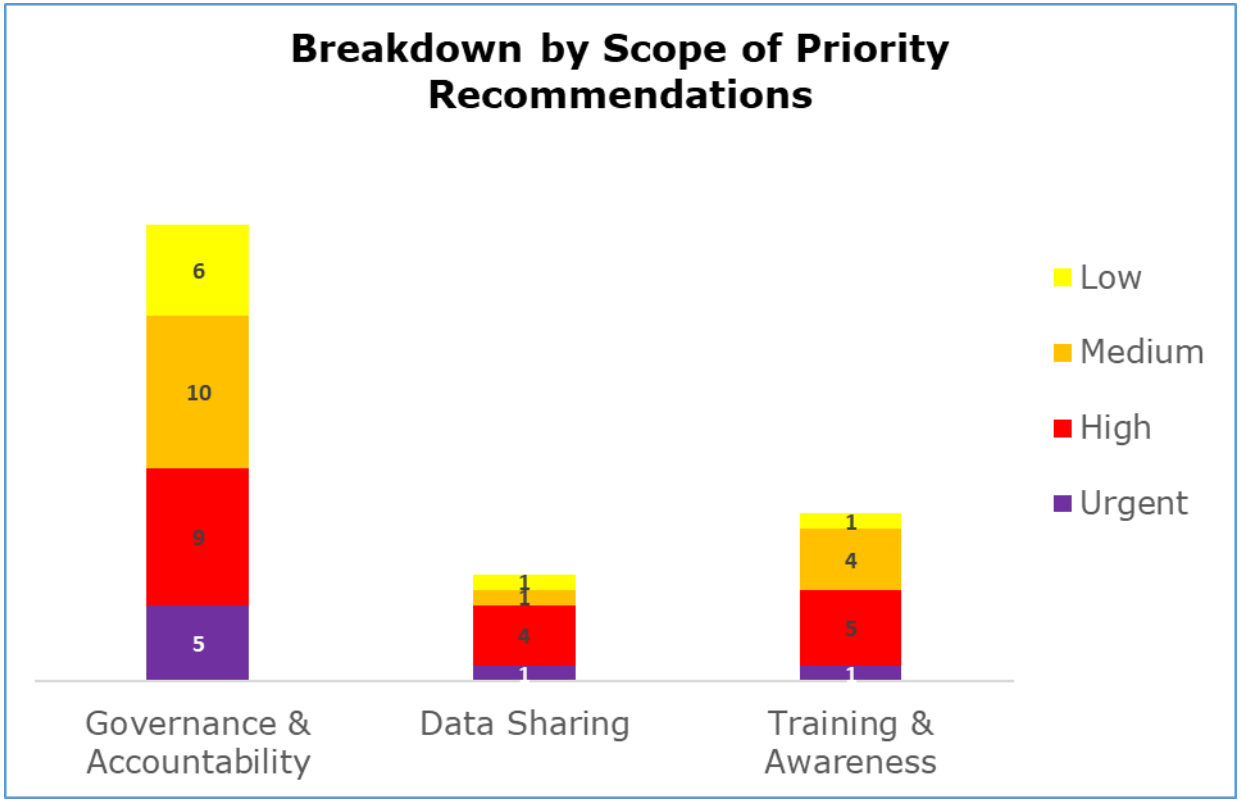
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist CCG in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. CCG's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Training and Awareness	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

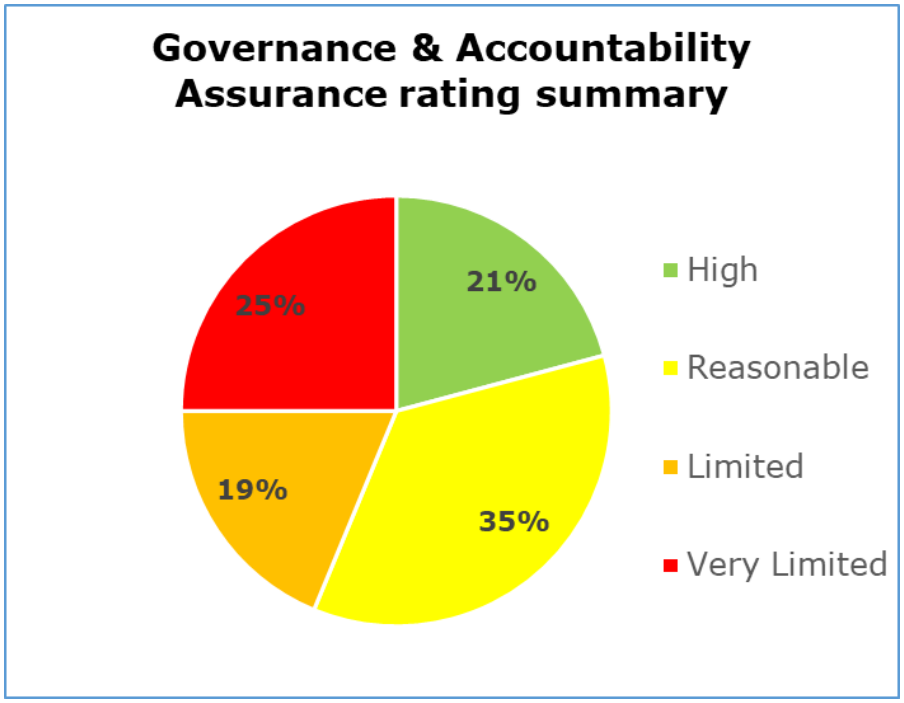
Priority Recommendations



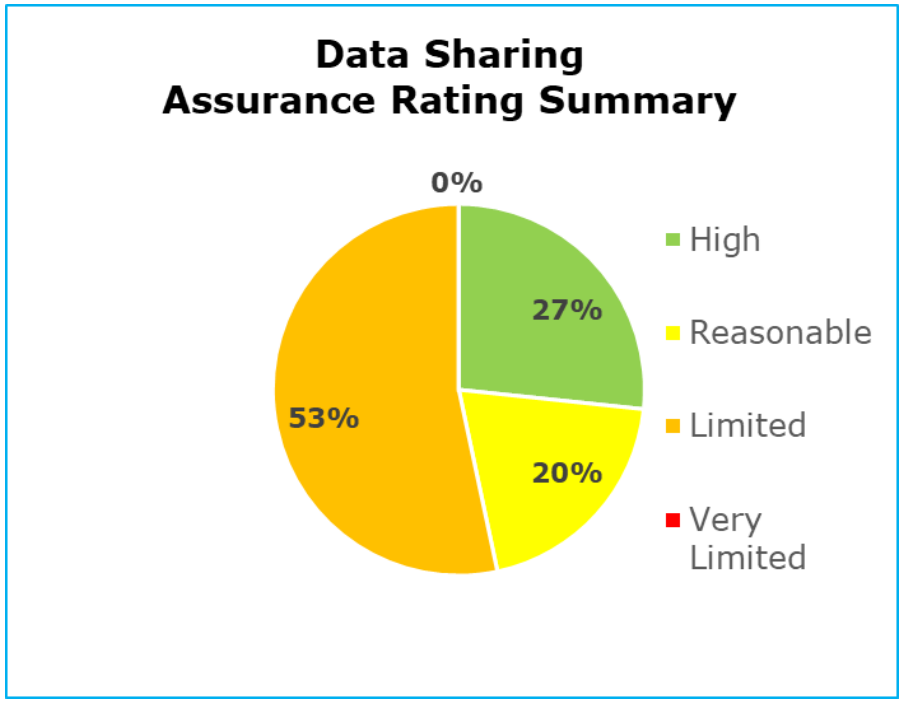
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 5 urgent, 9 high, 10 medium and 6 low priority recommendations.
- Data Sharing has 1 urgent, 4 high, 1 medium and 1 low priority recommendations.
- Training and Awareness has 1 urgent, 5 high, 4 medium and 1 low priority recommendations.

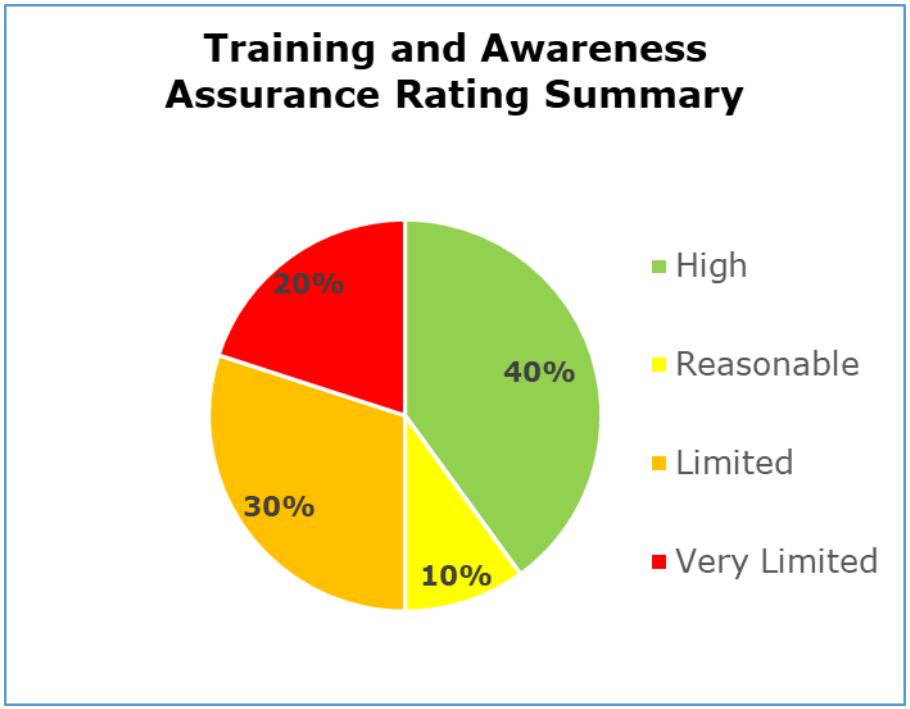
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 21% high assurance, 35% reasonable assurance, 19% limited assurance, 25% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 27% high assurance, 20% reasonable assurance, 53% limited assurance, 0% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Training and Awareness scope. 40% high assurance, 10% reasonable assurance, 30% limited assurance, 20% very limited assurance.

Areas for Improvement

Governance and Accountability:

- CCG do not have a fully documented information governance (IG) policy, framework and strategy, but work is already underway in this area, as CCG is in the process of reviewing and consolidating their newly expanded group's structure, systems, policies and processes.

- The flow of information between the senior management team, the Data Protection Officer (DPO), the audit and risk committee and other key IG committees and groups has not been finalised. Once determined, this should be fully documented and put into practice.

- Risk management has been identified by CCG as an area that requires further review and as part of this, CCG should consider implementing a process that ensures information risks are fully documented and managed throughout the organisation.

- There is no ongoing compliance monitoring of staff who are involved in the processing of personal information. Data protection policies and procedures should clearly set out how compliance with the data protection policy or procedure will be monitored.

- CCG are in the process of creating a central record of data processor contracts and a data processor procurement, due diligence and compliance process. CCG must ensure that an appropriate written contract is in place with each of its data processors. Once implemented, CCG will gain the required assurance and oversight of their data processors.

- A comprehensive, detailed data mapping exercise is required for all information assets and processing activities, to create an overarching record of processing activities (ROPA) which should then be reviewed on a regular basis. The exercise is key to complying with Section 61 of the DPA18 legislation and establishing the lawful basis for processing personal data, including special category and criminal offence data. This will help CCG to effectively update their privacy notices and create an Appropriate Policy Document.

Data Sharing:

- There is a lack of a documented process or procedure in relation to the sharing and disclosure of personal data, which may lead to inconsistencies in approach. A documented data sharing policy or procedure would promote a consistent approach to data sharing and reduce the opportunities for data to be shared inappropriately.

- CCG's privacy information does not meet all the requirements under Articles 13 and 14 of the UK GDPR. This means that data sharing activities are not fully documented and there is a lack of clarity around lawful bases for sharing. Therefore, CCG will need to review their privacy information to ensure that it meets the requirements within the legislation.

- Data sharing agreements put in place by CCG do not align with the ICO's data sharing code of practice. They do not define the processing relationship or include all of the necessary provisions, and a sizeable portion is dedicated to imposing requirements on the parties involved which are already imposed by Article 28 of the UK GDPR. CCG should amend its agreement template and revisit existing agreements to remedy this.

- Data sharing activities are not all reflected within CCG's ROPA, and data sharing agreements are not always correctly labelled within CCG's log of agreements. CCG will need to make improvements in this area to improve accountability.

- It has been noted that some members of staff regularly use a USB drive which is not encrypted to store personal data, albeit on a short-term basis. The ICO recommends that, where used, removable media is protected by technical security measures, such as encryption.

Training and Awareness:

- CCG should ensure staff do not have access to the personal data CCG processes before they have completed the data protection mandatory training. When staff fail to complete mandatory training, access to personal data should be removed until the necessary training has been completed. If staff begin to work with personal data before undergoing induction training, the organisation greatly increases the risk of a personal data breach.

- Ensure all staff, of all contract types, complete data protection training because this will decrease the risk of non-compliance and personal data breaches.

- CCG should regularly assess training needs and implement a Training Needs Analysis (TNA) for staff of all contract types to ensure compliance. CCG can then identify the necessary training needs of staff, which can then be met to maintain compliance with data protection regulations.

- CCG must ensure there is specified data protection training provided to the Senior Information Risk Owner (SIRO) to support their job role. This will significantly reduce the risk of non-compliance.

Best Practice

- CCG provide visual privacy notices in the form of YouTube videos, which are accessible from the privacy notices on the group's website. The visual privacy notice for students, in particular, was created in consultation with the student body. This features clear and simple information on who personal data is shared with and why.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Chichester College Group.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Chichester College Group. The scope areas and controls covered by the audit have been tailored to Chichester College Group and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.