Oakhill Secure Training Centre

Data protection audit report

July 2025

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 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 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 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 information responsibly, innovate and support economic growth.

In March 2024, the ICO developed a project to assess compliance with UK GDPR and DPA 2018 across the youth secure estate (YSE). Children in custody are held in one of four settings: young offender institutions (YOIs), secure children's homes (SCHs), a secure training centre (STC) or a secure school.

Secure Training Centre

Oakhill is the only STC in England and Wales. It provides secure placements for boys and girls between 12 and 18 and is managed by private organisation G4S under contract with the Ministry of Justice (MoJ). The centre provides full residential care, educational facilities and healthcare provision for children who are remanded by the court. These facilities are governed through the collaboration of multiple organisations, including the Department for Education (DfE), The Office for Standards in Education, Children's Services and Skills (Ofsted), the MoJ, the Youth Custody Service (YCS), and local authorities.

G4S manage and operate Oakhill and agreed to a consensual audit of its data protection practices.

Scope and Audit Approach

The scope areas covered by this project have been determined following an analysis of ICO intelligence which has highlighted data protection issues or risks within the sector. An auditing toolkit for this project has been created using a mixture of controls covering governance and accountability, cyber security and biometric recognition systems (BRS). This toolkit will be used on all audits across the YSE, however the findings from each audit are bespoke to each organisational structure and take into account the nature and extent of their processing of personal information.

This audit took place in May 2025 and followed the Information Commissioner's data protection audit methodology. The key elements of this were a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, and an inspection of physical controls. This report is addressed to Oakhill STC.

Reporting

This report contains non-conformities, recommendations, and good or best practice where appropriate. The intent of the report is to focus Oakhill's attention on those control areas requiring action to mitigate information risks and improve compliance.

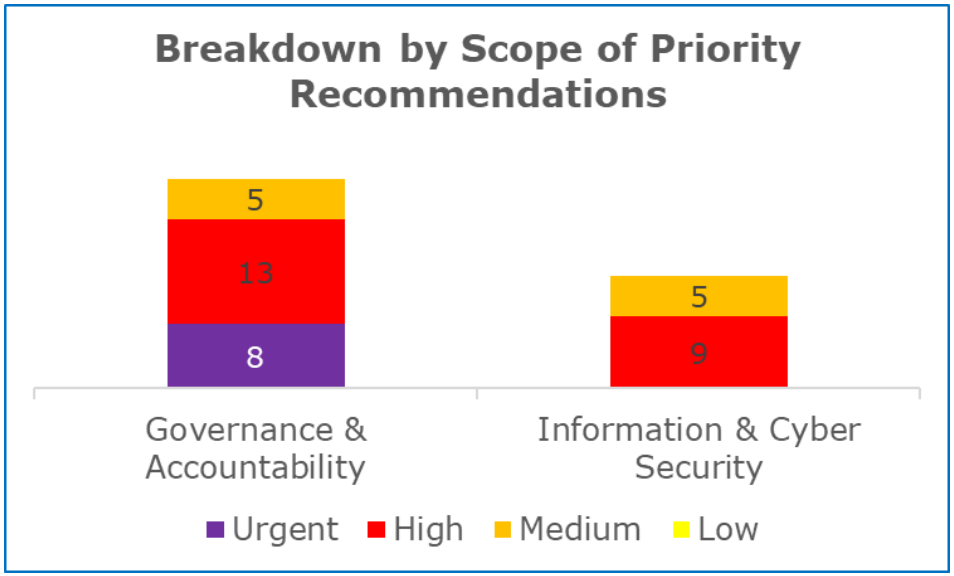
The ICO will use the findings from this project to identify and analyse common themes and patterns which would then be used to produce an outcomes report. These documents will be published on the ICO website and shared with the sector; however, individual organisations will not be identified in any outcomes report.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	**Limited**	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information and Cyber Security	**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 hybrid onsite and remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

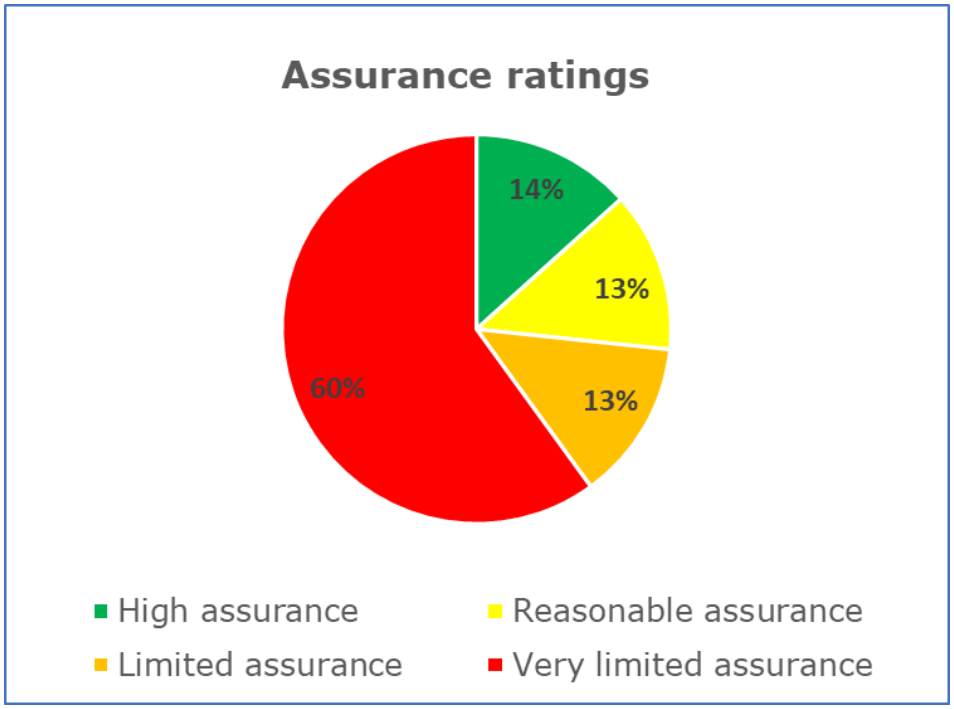
Priority Recommendations



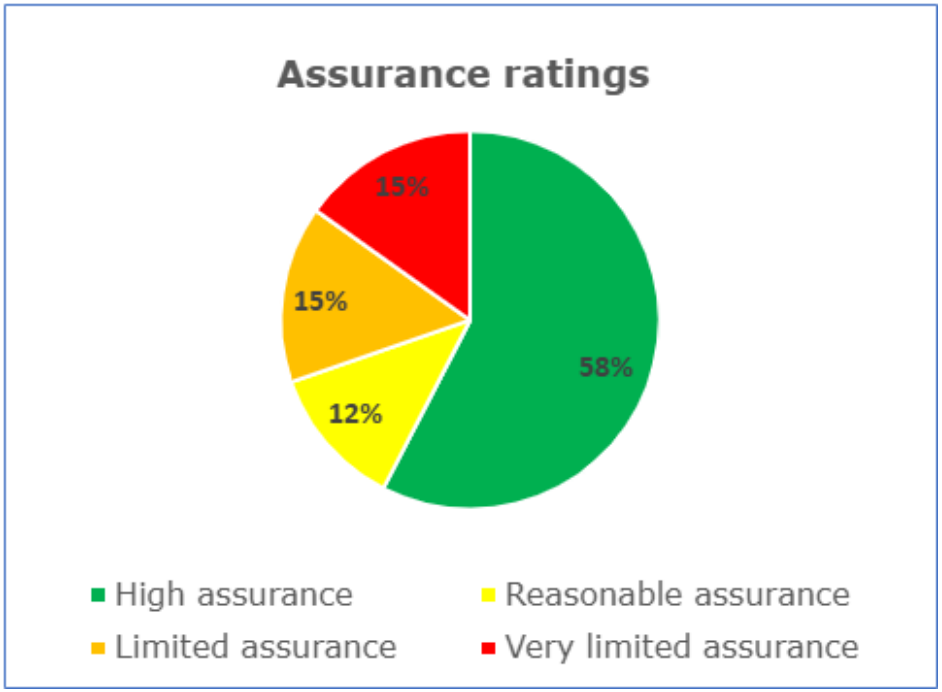
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- The Governance and Accountability scope area has eight urgent, 13 high and five medium recommendations.
- The Information and Cybersecurity scope area has nine high and five medium recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 14% high assurance, 13% reasonable assurance, 13% limited assurance, 60% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information and Cyber Security scope. 58% high assurance, 12% reasonable assurance, 15% limited assurance, 15% very limited assurance

Key areas for improvement

We identified some key areas within our audit, where Oakhill needed to implement further measures to comply with data protection law.

Governance and Accountability

- Continue efforts to establish Oakhill's responsibilities as either controller, joint-controller or processor for all personal information held and processed.
- Complete a comprehensive data mapping exercise to determine how personal information flows into, through and out of Oakhill. On determining responsibilities as controller, joint-controller or processor, create a Record of Processing Activities (RoPA) document that meets all legislative requirements. This should also accurately reflect all biometric data processing activities, including data sharing (DS) with third-party systems such as Kronos.
- Review the Data Protection Impact Assessment (DPIA) process at Oakhill to ensure that DPIAs are completed where required and meet the legislative requirements of the DPA18. Ensure DPIAs fully assess all DP risks and include mitigating measures required.
- Ensure that privacy information is given to children, visitors and staff to ensure they are suitably informed as to how their personal information will be processed and their rights regarding the processing.
- Clearly define and document the ownership of biometric data being processed. Ensure staff are appropriately informed of their responsibilities in ensuring the secure, access and compliant management of such data.

Information and Cyber Security

- Ensure physical access rights within Oakhill are periodically reviewed to provide assurance that staff and visitors have access only to areas and information that they require.

- Continue to progress the secure destruction of all laptops and hard drives currently held in storage. Ensure this process is formally documented.
- Update the data protection (DP) Record Retention policy to include clearly defined retention periods for biometric data. This should align with legal and regulatory requirements, as well as data minimisation principles under the UKGDPR and DPA18.
- Formally document the procedures for the secure transfer of personal information via physical media, including the use of postal services. This documentation should detail the security measures in place such as double sealing and signed for delivery and assign clear responsibilities for each step of the process.
- Establish a tailored and robust DS policy which clearly defines roles and responsibilities, outline acceptable DS practices, and include procedures for evaluating third-party DP measures.
- Conduct and document a DPIA for the collection and use of visitor biometric data, particularly its use in video call verification.

Key areas of assurance

At the time of the audit and based on the evidence seen by auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

Governance and Assurance

- Oakhill has a robust and clearly defined process for the management and reporting of personal data breaches (PDBs), which interviewed staff were aware of.
- Policies received as evidence are all version controlled, subject to regular review and owned by relevant senior staff.

Information and Cyber Security

- Clear desk and clear screen policies have been implemented within Oakhill.
- Oakhill carries out appropriate background checks on staff prior to being permitted access to personal information.
- A formal process is in place for assigning and revoking access rights for starters, movers and leavers.
- Appropriate password complexity rules have been applied to systems and applications processing personal information.
- Network vulnerability scans are routinely conducted, and appropriate remedial actions are implemented to address any identified risks.

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 Oakhill Secure Training Centre.

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 Oakhill Secure Training Centre. The scope areas and controls covered by the audit have been tailored to Oakhill Secure Training Centre and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.