Follow-up of *Managing child safety information*

Report 20: 2018–19

Queensland Audit Office
Better public services

Queensland
Audit Office
Better public services

Your ref:
Our ref: 9182P

29 May 2019

The Honourable C Pitt MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Speaker

Report to parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled *Follow-up of Managing child safety information* (Report 20: 2018–19).

In accordance with s.67 of the Act, would you please arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Brendan Worrall
Auditor-General

Contents

Audit objective and scope

Objective

In this follow-up audit, we assessed whether the Department of Child Safety, Youth and Women has effectively implemented the recommendations we made in *Managing child safety information* (Report 17: 2014–15). We also assessed whether the actions taken have addressed the underlying issues that led to our recommendations in that report.

Scope

In *Managing child safety information* (Report 17: 2014–15) we audited the former Department of Communities, Child Safety and Disability Services, which was responsible for administering the *Child Protection Act 1999.*

Following machinery-of-government changes in December 2017, the Department of Child Safety, Youth and Women assumed responsibility under the *Child Protection Act 1999* for protecting children and young people in Queensland. To avoid confusion, we refer to both the Department of Communities, Child Safety and Disability Services and the Department of Child Safety, Youth and Women as 'the department' throughout this report.

In conducting this follow-up audit, we also engaged with:

- some non-government organisations funded (by the department) to provide family support and child protection services
- the Department of Education
- the Department of Health
- the Queensland Police Service.

Appendix B has more information about our audit objectives and methods.

Assessing implementation

We assessed whether each recommendation has been fully implemented, partially implemented, not implemented, or is no longer applicable. The definition for each status is provided in Appendix B.

Performance audit on Queensland's family support and child protection system

The Queensland Audit Office is also undertaking a performance audit of the family support and child protection system in Queensland.

The objective of that performance audit is to assess how effectively Queensland government agencies are working together for the safety and wellbeing of Queensland children. We will table the results of that audit in parliament in 2019–20.

Key facts

Government agencies and non-government service providers work together to protect children in Queensland

The Department of Child Safety, Youth and Women has primary responsibility for protecting children who have been harmed or are at risk of harm and do not have a parent willing and able to protect them.

In 2017–18, the Department of Child Safety, Youth and Women received 119 192 reports about concerns of harm or risk of harm to a child.

Source: Department of Child Safety, Youth and Women website.

9 093 children lived in foster care, kinship care or residential care services in Queensland at 30 June 2018.

Source: Department of Child Safety, Youth and Women 2017–18 annual report.

188 non-government organisations are funded to provide family support and child protection services, including running residential care facilities for children.

Source: Department of Child Safety, Youth and Women (at February 2019).

$1.07 billion was spent in Queensland on family support and child protection services in the 2017–18 financial year.

Source: Report on Government Services 2019.

Introduction

All organisations that provide services to vulnerable children and their families collect, record, maintain, and share a range of personal and sensitive information to support child safety functions. We refer to this as ‘child safety information’.

Under the *Information Privacy Act 2009*, all Queensland government agencies must protect personal information they hold against loss, unauthorised access and other misuse.

However, the *Child Protection Act 1999* requires government and non-government organisations to share child safety information in order to effectively protect and care for children and promote their wellbeing. In doing so, they must respect the privacy of individuals to the greatest extent possible and ensure the information that is shared is properly used, stored, retained, and disposed of.

Government and non-government agencies need to collaborate and share information quickly, easily, and securely to ensure the right services are being provided at the right time.

Achieving the balance between making information accessible when it is needed but keeping it secure at all times is a challenge for the department and the organisations with which it works to protect children and young people in Queensland.

Report 17: 2014–15

In *Managing child safety information* (Report 17: 2014–15) we examined whether child safety information was secure, yet available to authorised people who provide child safety services.

The audit focused on information management for services provided by the department and non-government organisations to children in need of protection, including out-of-home care. We examined:

- accessibility of information—to determine whether government and non-government organisations were efficiently sharing accurate child safety information
- security of information—to determine whether agencies had appropriate physical and computerised security arrangements to maintain confidentiality of information.

The audit assessed the level of collaboration between government and non-government organisations. We audited the department and three non-government organisations.

We concluded

The department did not have the right balance between security and accessibility of child safety information. More specifically, we concluded that while it adequately secured child safety information internally, it was not regularly reviewing user access to its systems that stored sensitive data. Ready access to necessary child protection information was problematic for agencies and service providers. Information sharing with other government and non-government organisations in the child safety service chain was neither efficient nor secure and a lack of data integrity meant the department could not easily collect accurate information to report on service outcomes.

We found

Accessibility of child safety information

The department invested significant resources in implementing information systems for its internal use but did not assess or review requirements of new technology to support changing business needs. It was slow to address the information requirements of its service providers.

Its case management system was not designed to share information across multiple service providers, which resulted in significant duplication of effort within the child safety service chain. The lack of integrated systems meant information from the service providers about the wellbeing of children was not easily accessible to the department. Determining which system had the correct information was difficult, and analysing information to monitor overall trends in service outcomes was a time-consuming exercise.

Technology limitations, different interpretations of child safety practices and a tendency for people to be cautious when sharing information with other organisations meant that critical information was, at times, not available when needed.

Because of the disparate information systems used by various child safety service stakeholders, there was duplication of effort and a lack of data integrity. Without a single accurate data source, the department could not easily collect information and report on service outcomes.

Information security

The department had risk management practices in place, with senior management oversight and monitoring of information technology risks.

It had implemented good controls to secure the main information systems used to manage child safety information. But system limitations meant information was often extracted from systems into spreadsheets, which could then be accessed by people who were not authorised to access the information systems.

Because the department was not reliably updating access to its information systems, some staff retained access to child safety information when they no longer needed it.

Stakeholders in the child safety service chain used emails to send and receive sensitive information, which risked unintentional disclosure to third parties if sent to the wrong email address.

The department also risked inappropriate disclosure of data because it allowed sensitive information to be downloaded and shared using removable media and mobile technology. It did not set minimum information security standards on how to protect child safety information that exists in electronic form for its service providers. It also did not offer guidance on how to manage security risks when using outsourced services or Cloud service providers.

We recommended

Figure A summarises the six recommendations we made to the department. It accepted all of them.

Figure A
Recommendations in *Managing child safety information* (Report 17: 2014–15)

We recommend that the department:	
Accessibility of child safety information	
1	develop and implement a co-ordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain
2	implement contemporary information systems
3	use information available across organisational boundaries within the service chain to gain insights and improve service outcomes
Security of child safety information	
4	specifies the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system
5	improves security within the existing environment
6	develops security standards for service providers. These standards should be included in service agreements.

Appendix C contains further detail on the six recommendations we made in Report 17: 2014–15.

Summary of audit findings

The department has made progress towards implementing most of the six recommendations. We assessed that one is fully implemented and five are partially implemented.

Figure B details the recommendations and our assessment of their implementation status.

Figure B
Implementation status

Accessibility of child safety information (Chapter 1 in this report)	
1. Develop and implement a coordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain. QAO assessment: *Partially implemented*	
The department has:	The department still needs to:
• published its *Information sharing guidelines* to support changes to information sharing provisions in the *Child Protection Act 1999* • implemented an internal data governance framework • developed the *Child and Family Business Systems Strategy 2018–2022* • begun a program of work to replace the Integrated Client Management System (ICMS), its main system for storing child safety information, including completing internal high-level modelling of information flows.	• continue to conduct collaborative planning for information requirements between the department and key stakeholders across the child safety service chain • bring the existing information systems and requirements of all key stakeholders together in a coordinated holistic information management model.
2. Implement contemporary information systems. QAO assessment: *Partially implemented*	
The department has:	The department still needs to:
• developed and implemented new information systems which improve access to information for child safety purposes • developed internal performance and monitoring reports using Power BI • developed and started rolling out iDocs, an electronic records management system • begun an ICMS replacement program (with full implementation expected June 2023).	• continue to implement contemporary information systems that allow appropriate access to relevant information held across government.

Accessibility of child safety information (Chapter 1 in this report)

3. Use information available across organisational boundaries within the service chain to gain insights and improve service outcomes.

QAO assessment: *Partially implemented*

The department has:	The department still needs to:
• begun annual public reporting on the progress of its *Supporting Families Changing Futures* reform program, including initiatives undertaken across government • updated its memorandum of understanding (MOU) with the Department of Education to focus on the two agencies achieving the best possible education outcomes for children • begun reporting against key outcome areas agreed in the MOU with the Department of Education • established quarterly director-level meetings with the Department of Education aimed at improving the participation of children in care in education and at ensuring those children receive education support • improved the quality and completeness of data in the ICMS that is made available to appropriate people external to the department to view.	• improve its approach to using information available across organisational boundaries from relevant government agencies and non-government service providers to gain insights and improve service outcomes • improve system-wide analysis and reporting on trends, emerging issues, and performance • conduct data matching in accordance with the key outcome areas agreed in the MoU between its system and the Department of Education's system • ensure the cross-agency meetings (to develop and coordinate strategies and programs aimed at improving the educational outcomes for eligible children) occur with greater frequency and consistency.

<table>
<tr><th colspan="2">Security of child safety information (Chapter 2 in this report)</th></tr>
<tr><td colspan="2"><b>4. Specify the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system.</b>
QAO assessment: <i>Fully implemented</i></td></tr>
<tr><td>The department has:</td><td>The department still needs to:</td></tr>
<tr><td>• ensured that security risk assessments have been completed for all new systems
• ensured that efficient exchange of information is specified in the business cases and design processes for all new systems.</td><td>• as business as usual, continue specifying the efficient and secure exchange of information as a key business requirement when selecting new systems or revising existing systems.</td></tr>
<tr><td colspan="2"><b>5. Improve security within the existing environment</b>
QAO assessment: <i>Partially implemented</i></td></tr>
<tr><td>The department has:</td><td>The department still needs to:</td></tr>
<tr><td>• introduced penetration testing for existing systems (which determines whether the security of the system can be breached)
• developed cyber security plans for new systems
• provided mandatory training for its staff on information privacy and security at induction
• implemented an encrypted email service
• amended the way it logs use of USB devices to show if a departmental-approved encrypted USB device is used
• completed (in January 2019) a state-wide review of ICMS access.</td><td>• provide mandatory refresher training for all staff on information privacy and security
• conduct regular reviews of user access levels of all information systems used to store and manage child safety information
• mandate the use of secure communication channels when sending child safety information and provide further training on the use of the encrypted email service.</td></tr>
<tr><td colspan="2"><b>6. Develop security standards for service providers. These standards should be included in service agreements.</b>
QAO assessment: <i>Partially implemented</i></td></tr>
<tr><td>The department has:</td><td>The department still needs to:</td></tr>
<tr><td>• obtained legal advice on the privacy impacts of its Advice, Referrals and Case Management system used by non-government organisations that provide early intervention family support services
• started monitoring service providers' compliance with information privacy and security obligations through:
– audits of the <i>Human Services Quality Framework</i>
– inspections of licensed care providers.</td><td>• provide mandatory minimum security standards for service providers
• include the security standards in service agreements
• adopt a more systematic and proactive inspections and monitoring framework of service providers' compliance with the security standards
• provide greater guidance to staff conducting inspections.</td></tr>
</table>

Source: Queensland Audit Office.

Further detail on the actions taken and further work needed is provided in the following chapters.

Audit conclusions

The department has not effectively implemented all of the recommendations we made in *Managing child safety information* (Report 17: 2014–15). It has taken steps to implement the recommendations and to address some of the underlying issues. It has made progress in improving access to information but not in a holistic manner and security is still an area needing further work.

Through several initiatives, including implementing new information systems for collecting, recording, maintaining and sharing child safety information, the department has made accessing some information easier and more user-friendly for its own staff, non-government service providers and carers.

However, child safety information held across various parts of the family support and child protection system is still almost completely unintegrated. Automated information exchange between stakeholders, where it does occur, is limited. There are plans for making the most significant child safety system change—replacing the Integrated Client Management System (ICMS)—but it has not happened yet. This will involve considerable effort and investment.

The department has implemented more secure means of information exchange, but they are not well used by department staff. It needs to do more to safeguard the security of information in its systems and in how it exchanges information with non-government service providers.

At present, the considerable information available across organisations within the family support and child protection system is still not used as effectively as it could be to provide insights and improve outcomes for children in Queensland.

1. Accessibility of child safety information

This chapter covers progress made by the Department of Child Safety, Youth and Women (the department) in making child safety information more accessible across the child safety service chain.

Coordinated model for information management and sharing

We recommended that the department develop and implement a coordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain.

Status: **Partially implemented**

In 2015, we found that the department lacked strategic direction in dealing with the evolving information requirements of all organisations that provided services to vulnerable children.

It had invested significant resources in implementing information systems for its own use but was slow to address the information requirements of its service providers. It was also not continually assessing new technology to support changing business needs.

We concluded that collaborative planning was needed for information requirements between the department and key stakeholders across the child safety service chain, particularly while implementing recommendations from the Queensland Child Protection Commission of Inquiry's *Taking Responsibility: A Roadmap for Queensland Child Protection* report and other child safety service reviews.

Progress made

While there is work still to be done, the department has made progress in addressing the issues that led to our recommendation. It has:

- published its *Information sharing guidelines* to help government and non-government organisations providing services to children and families understand changes to information sharing provisions in the *Child Protection Act 1999*
- implemented a departmental data governance framework
- begun a program of work to replace the Integrated Client Management System (ICMS), its main system for storing child safety information, including completing high-level information modelling and planning documents.

Changes to legislation and guidelines

In October 2018, the *Child Protection Act 1999* was changed to make it easier for government and non-government organisations that deliver services to children and families to share information with each other. The changes allow more information to be given to:

- children and young people who are/have been living in care
- parents and guardians
- the Queensland Police Service
- child welfare authorities in other jurisdictions.

At the same time, the department published its *Information sharing guidelines* to help stakeholders understand the legislative changes and what information they can share and when. It also updated its internal *Child Safety Practice Manual* to align with the changes to the *Child Protection Act 1999*.

Data governance model

In April 2018, the department introduced a data governance framework. The framework's purpose is to increase confidence in data that the department relies on to protect children and young people. It outlines the roles and responsibilities of officers as well as quality, uses, sources, classification and life cycle requirements for data. It also includes a 'decision tree' to aid staff in deciding when it is appropriate to release child safety information.

ICMS replacement program

In 2015, the department began a program of work to replace its main system for storing child safety information, the ICMS. The intent of the program is to provide the department with the ability to easily see all relevant information about a child and for agencies and funded service providers to access and contribute to this information. Something which the ICMS is currently not able to do.

In May 2018, the department developed a high-level model under its ICMS replacement program showing what it described as future information flows between itself and stakeholders.

The model did not identify gaps in:

- information sharing that occurs between stakeholders not involving the department
- information flows across the entire child safety service chain.

For example, the model does not show that information sharing between the department and the non-government organisations providing services for children in care is not automated and is currently conducted outside of an information system. The department and its service providers mostly use unsecured email to share child protection information.

The department's *Child and family business systems strategy 2018–2022* documents its plan for information management and sharing. It identifies the information systems that will be used to manage and share information between key stakeholders in the child safety service chain. Again, it is a high-level document that does not include information management and sharing across the entire child safety service chain.

What still needs to be done

While these changes have resulted in some improvement in information sharing, they do not provide a coordinated model that comprehensively addresses information management and sharing across the entire child safety service chain.

To do that, the department needs to complete a detailed assessment of information requirements and collaboratively plan with all stakeholders to meet these requirements. It will need to include the multiple initiatives already implemented and bring the information systems of all key stakeholders together in a holistic information management model.

Contemporary information systems

We recommended that the department implement contemporary information systems that:

- integrate the information that is held across all parts of child safety services
- automate information exchange with authorised persons
- are flexible and adaptable to changes in business processes
- provide relevant functionality and reporting
- enable the collection of relevant information and promote outcomes-based reporting
- make it easier to manage multiple records on the same client within different media and in different formats.

Status: **Partially implemented**

In 2015, we found that the department had not integrated its systems to record and share information with its service providers. Its systems did not allow its officers to record events as they happened or to access information on an anywhere/anytime basis.

Because the systems were not designed for collaboration and information sharing, information was exchanged using emails, and documents were printed for physical files. Disparate systems, coupled with a reliance on physical files, meant that some information held in the systems was inconsistent and out of date.

There was limited capacity to meet changing business requirements because the ICMS had complex infrastructure and ageing technology. Because of this, people had trouble accessing information and were managing information outside of key systems.

For example, the department recorded information in the ICMS but could not share it with service providers. Service providers then recreated subsets of the same information in their own systems in electronic and physical forms.

The ICMS did not have the ability to verify performance data reported by service providers and monitor outcomes. As a result, staff kept spreadsheets outside of the system. These spreadsheets lacked the necessary controls and security to adequately protect such sensitive information.

Internal performance reporting within the department was complex, time consuming and needed significant resources from two separate teams. Consequently, departmental regional offices adopted their own reporting processes, which were inconsistent and varied in quality.

Progress made

While the department plans to replace the ICMS, it has not yet done so. The ICMS is still the department's main information system for collecting, recording and maintaining child safety information.

The department has implemented new information systems and applications (apps) for collecting, recording, maintaining and/or viewing child safety information, including:

- the Our Child system
- the CSXpress, Carer Connect and Kicbox apps
- the Advice, Referrals and Case Management system
- CourtShare
- the internal electronic documents records management system (iDocs).

The systems and apps have partly addressed some of the underlying issues we reported in 2015. But as they do not address all the issues, the department has not yet fully implemented the recommendation.

ICMS

Significant resources are spent maintaining and upgrading the ICMS. The technology is reaching the end of its useful life and integration with new technologies is becoming increasingly complex.

In March 2017, the Queensland Family and Child Commission, in its *Strengthening capacity across Queensland's child protection system* report, stated that the ICMS was outdated. It recommended it be replaced with a modern, integrated client management information system.

The department has a program of work underway to replace the ICMS. A detailed business case for the program was finalised by its program board in February 2019 and in-principle funding was approved by Cabinet for the first tranche of work. Full implementation is expected by June 2023.

Our Child

The Our Child system was developed in response to issues identified in the Queensland Family and Child Commission's report *When a child is missing: Remembering Tiahleigh – a report into Queensland's children missing from out-of-home care.*

It is an information sharing portal used to view information contained in the information systems of the department (in Child Safety Services and Youth Justice Services), the Department of Education, Queensland Health and the Office of the Public Guardian.

Currently, Our Child can only be used in very specific circumstances—when a child in care has been reported missing to the Queensland Police Service. Authorised departmental and Queensland Police Service officers can log into the portal to view information about agencies' recent interactions (if any) with the child, for example, to find out if the child had attended school.

The department advised us that it intends in the future to use this platform to increase information sharing capability across government.

Mobile applications

Across 2017 and 2018, the department implemented three apps (CSXpress, Carer Connect and Kicbox) that allow users to view and upload information electronically for different purposes.

- **CSXpress**

Using their departmental mobile device when out of the office, the department's child safety officers use the CSXpress application to view information about children and young people they case manage, which is stored in the ICMS. At present, 87 per cent of officers have access to mobile devices.

- **Carer Connect**

Carer Connect is an application that provides foster and kinship carers with access to ICMS information through their personal computers and mobile devices. It includes some health and education records, authority to care forms, emergency contact details, and child support networks. Nearly 1 000 carers have registered to use the application.

These applications make it possible for departmental staff and carers to access and upload some information on mobile devices. This is an important step in making child safety information more easily accessible while maintaining its security.

- **Kicbox**

Kicbox is an application that allows child safety officers and carers to communicate with children in care using private messaging. The child can upload photos and post memories and milestones. Carers and child safety officers can add documents such as birth certificates and authority to care documents. Almost 500 children have active Kicbox accounts. Child safety officers reported to us that children were not regularly using Kicbox because they can't use it to connect with their friends.

Advice, Referrals and Case Management system (ARC)

The department implemented ARC for use by non-government organisations that provide early intervention family support services. Service providers use the system to create and save case notes, assign tasks to workers and track workers' caseloads.

While organisations are not able to directly access the information of any other organisation within the ARC system, they are able to use it to share information with another service provider when they have the consent of the family receiving the service. An example of this is when a family moves to another location and wishes to continue receiving the service.

ARC allows some automated information exchange between service providers and has a reporting functionality.

Service providers use ARC's reporting functionality to run performance reports that have the information they need to report to the department under their service agreements. But ARC does not interface with the OASIS system—the system the department requires service providers to use to report their performance.

Instead, service providers must manually re-enter information from their ARC system-generated performance reports into OASIS. Not only is this an inefficient process, it also introduces the possibility of data entry errors. Service providers have also told us they find it difficult to reconcile the data produced in the auto-generated reports with their own records. The department has a project underway to replace OASIS in 2019.

The department cannot access information stored in ARC about individual cases because it considers it to be personal information collected by the service provider. The service provider must comply with the Information Privacy Act and keep the personal information confidential. Service providers cannot use ARC as a means of sharing information with the department.

However, the department can generate de-identified aggregated information from ARC data for reporting purposes including:

- number of referrals received by non-government organisations
- source of referrals (for example, Queensland Police Service, health professionals, education professionals)
- response type.

CourtShare

In October 2018, the department implemented the CourtShare system. It allows departmental officers to work collaboratively with the Office of the Director of Child Protection Litigation to manage child protection order applications and proceedings in the Children's Court. The system manages the end-to-end process of applying for child protection orders. Records stored in CourtShare are accessible to both agencies.

CourtShare has improved the efficiency of information sharing by allowing child safety officers to access information in a timely manner, for example, court documents that are uploaded by the Office of the Director of Child Protection Litigation.

Updates to CourtShare in April 2019 provided some integration with ICMS, reducing some manual data entry of CourtShare records into multiple departmental systems. Full integration with ICMS is not expected until completion of the ICMS replacement program, expected in 2023.

iDocs

The department has started rolling out its new internal electronic documents records management system (iDocs) to its offices. All documents that departmental officers currently save into the ICMS, for example, case plans for children in out-of-home care, will be stored in iDocs in future.

iDocs has been designed to make it easier for departmental officers to manage and access documents, and includes a direct link to documents from ICMS records. Full implementation is expected by the end of February 2020.

Reporting Capabilities

The department uses Power BI to create dashboards and display data to meet a variety of user requirements within the agency. For example, Power BI produces reports on the numbers and sources of referrals to family support services from data in the ARC system.

What still needs to be done

It takes a lot of time to effectively replace significant systems like the ICMS, and the department still has considerable work to do in achieving this. It expects to be finished by June 2023.

The Our Child system shows that, despite government agencies using different systems, there is technology available that could allow appropriate access to information held across government about a child. Participating agencies are discussing how the Our Child technology could be used more broadly to make information sharing more effective and efficient.

The introduction of Our Child, ARC, CourtShare, and the other applications represent an improvement in information sharing but are only available to select subsets of agencies and service providers. For example, non-government organisations providing support services for children in care currently use their own systems to record and store child safety information.

The department needs to continue to introduce contemporary, connected information systems across government that allow appropriate broader access to information to ensure vulnerable children are protected and their care needs are met.

Also, privacy, confidentiality, security, diverse legislative requirements and different agency approaches to risk still pose barriers (actual and perceived) to broader information sharing across the child safety system. The department needs to overcome these barriers as part of any information systems improvements for the systems to be effective.

Gaining insights using information across organisational boundaries

We recommended that the department use information available across organisational boundaries within the service chain to gain insights and improve service outcomes. For example, to:

- verify whether children not recorded as attending schools are really not attending schools and implement plans for their educational support
- implement effective measures to address school attendance, suspension, exclusions, absences and abscondments to evaluate the success of its partnership with the Department of Education
- monitor all aspects of child safety services including those where the responsibility is devolved to other government departments
- establish regular monitoring processes for education support plans, health passports and transition plans
- implement mandatory recording of reference keys for the Integrated Client Management System and OneSchool to ensure that information on the same child is being recorded correctly and consistently in the two systems
- implement measures to improve and monitor the completion and timeliness of information about transition arrangements within the case plans and transition from care plans.

Status: **Partially implemented**

In 2015, we found that the department was unable to readily draw on the broad range of information held across the child safety system to assess outcomes for children and gain insights.

Information systems across the government and non-government organisations that provided services to children in care were not integrated. It was time consuming to match data held by the different organisations to confirm its accuracy and difficult to aggregate individual case-based information.

This meant the department could not easily produce reports on the outcomes of services provided to children in care. This limited its ability to take a more strategic approach to child safety services.

Progress made

The department has made some progress towards implementing our recommendation but is still unable to access and use much of the information held across government agencies and non-government service providers to gain insights and improve outcomes for children.

Reporting performance of the family support and child protection system

In 2016, the department began annual public reporting on the progress of the *Supporting Families Changing Futures* reform program. This is based on more detailed annual reporting to government.

These annual reports include information about initiatives undertaken across government to implement the reforms from the Queensland Child Protection Commission of Inquiry.

The reports draw on the department's performance data and include evidence that the department is using the data to gain insights on discrete components of the family support and child protection system. For example, the *Supporting Families Changing Futures 2018 Update* identifies that a large proportion of reports to the department from mandatory reporters do not meet the threshold for investigation, and that more needs to be done to raise awareness of family support services.

The department reports on some activities and services provided by other government and funded non-government agencies, such as the level of engagement in family support services and the rates of children returning to the system.

Sharing education information and reporting on outcomes

Memorandum of understanding with the Department of Education

In 2016, a memorandum of understanding (MOU) between the department and the Department of Education was amended to focus on the agencies achieving the best possible education outcomes for children. The MOU includes the agencies:

- working cooperatively and collaboratively to improve accountability, reporting options and sharing information for the life outcomes of relevant children, and sharing data required to support and monitor children's education outcomes
- reporting against targets for key outcome areas, including school attendance, suspension, exclusions and absences
- identifying current and emerging issues in relation to the educational support needs of eligible children and developing strategies to improve coordinated service responses by the agencies
- meeting on a regular basis to develop and coordinate strategies and programs aimed at improving the educational outcomes for eligible children.

While the two agencies have set up initiatives and processes to deliver on the MOU agreed actions, most are not being done in the way intended or as often as intended. This limits their effectiveness in helping the department to gain insights and improve service outcomes for children.

To report against the targets for key outcome areas agreed in the MOU, the agencies must match their individual data. This enables them to identify the children to be included in their reporting and ensure the data is accurate. The data matching exercise has only occurred once a year since 2016 and produces only an aggregate-level report, with no information about individual children included. Prior to 2015, data matching occurred quarterly.

The aggregated attendance data the department receives from the Department of Education as part of the data matching process includes only children in care who are enrolled in school full-time. The department uses this information to track the overall attendance of children in care, but the department cannot easily monitor the overall trend of school attendance by all children in care.

Cross-agency meetings

In February 2017, the department and the Department of Education set up cross-agency director level meetings to discuss children in care participating in education and education support plans (which all children in care must have to receive the education support funding for which they are eligible).

However, the agencies only had four meetings in the 2017 and 2018 calendar years despite the group's terms of reference providing for quarterly meetings.

The agencies decided at the September 2018 meeting that they would form working groups to target participation of children in care in education and education support plans. Both working groups are yet to meet, and membership is still to be finalised.

Another cross-agency group, which includes the department and the Department of Education, is the Student Protection and Reporting Advisory Committee. The Queensland Police Service is the other member of the committee.

Formed in September 2016, the Student Protection and Reporting Advisory Committee's purpose is to provide governance across student protection reporting enhancements involving changes to the three agencies' systems and business processes. In October 2018, the committee discussed developing greater access to the Department of Education's OneSchool data, but this has not yet occurred.

Monitoring education support plans, health passports and transition plans

Child safety officers monitor whether education support plans and health passports (which contain information about the health needs of a child) have been created. They also have to complete plans for a child's transition to independence.

In August 2018, the department undertook a project to update ICMS data and ensure it was accurate before launching the Our Child system and its CSXpress and Carer Connect apps. It generated weekly reports detailing the ICMS data that would be used by the new systems and sent them to regional offices so they could check the accuracy and completeness of the data. Hundreds of education support plans and health passports were added to the records of children in the ICMS as a result, which means it had not been kept up to date.

The department's reporting team now generates monthly reports for each of its regions that identify discrepancies in education data recorded in the ICMS, for example, records that identify a child as being eligible for an education support plan without having a plan attached.

The department is working with other departments and Commonwealth government agencies to aid transition and information exchange for the National Disability Insurance Scheme and the My Health Record.

What still needs to be done

The department still needs to improve its approach to using information from government and non-government organisations providing services to vulnerable children to assess outcomes and gain insights.

Performance analysis and reporting should not be agency specific or limited to discrete components of the family support and child protection system. System-wide performance analysis and reporting would enable the agencies to be proactive and responsive to emerging issues before they escalate.

The Inter-Departmental Committee (which the department co-chairs) is responsible for overseeing reforms, to increase the use of information across government and non-government service providers. It needs to define what the system-wide approach will be for analysis and reporting on trends, emerging issues and performance.

The department and the Department of Education should renew their focus on working together to achieve the best possible education outcomes for children and ensure the initiatives or processes set up to deliver on their MOU commitments continue to happen. As part of this, there should be:

- more frequent data matching and reporting in accordance with the key outcome areas agreed in the MOU between the department and the Department of Education
- more frequent and regular cross-agency meetings to develop and coordinate strategies and programs aimed at improving the educational outcomes for children.

2. Security of child safety information

This chapter covers progress made by the Department of Child Safety, Youth and Women (the department) in strengthening the security of child safety information.

Security of information in new systems

In 2015, we recommended that the department specify the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system.

Status: **Fully implemented**

In 2015, the department's systems for recording and managing child safety information were not designed for sharing and collaborating with other government agencies or service providers. This meant that sensitive child safety information was exchanged using non-secure means, including email and printed documents for physical files.

Progress made

The department included efficient and secure exchange of information as a key business requirement when it selected and designed the new information systems it has introduced since 2015.

The department included security planning in the solution planning process and completed security risk assessments for each of the new information systems. It has incorporated security planning (including consideration of mandatory security controls) in its standard design documentation and as an integral part of its information solution design process.

The department follows the Queensland Government's information and communication technology project management processes, including using risk management techniques to ensure the appropriate security capabilities are part of new information services.

Security of information in existing systems

We recommended that the department improve security within the existing environment by:

- extending secure email services in the current system to encrypt information exchange with all service providers
- identifying where sensitive child safety information is stored in the file system and ensuring access controls are authorised by business owners
- reviewing and updating user access levels regularly for key child safety systems
- preventing transfer of sensitive child safety data from the departmental network to unencrypted, removable media (such as USB memory sticks).

Status: **Partially implemented**

Inappropriate access to, or disclosure of, child safety information can pose grave risks to the safety and wellbeing of a child. All organisations supporting children must keep personal information confidential and restrict access to case data.

In 2015, we found that sensitive child safety information was being exchanged with service providers by email and unencrypted media and mobile devices. This increased the risk of intentional and unintentional loss, theft, and/or disclosure of sensitive information.

We also found that the department had well-designed system controls to restrict system access to authorised persons. However, these controls were undermined by a lack of review of user access. We found staff who no longer needed access to child safety information systems still had approved access.

Progress made

Since the audit, the department has put in place an encrypted email service, created cyber security plans for new systems, and provided some training to its staff in managing data securely. However, it has made limited progress in addressing most of the underlying issues that led to our recommendation.

Encrypted email service

Email is still the main way the department exchanges child safety information with non-government organisations providing services to children in care. This is because it has not established information exchange systems to securely manage its exchange of child safety information.

Since the audit, the department has introduced an email service that its staff can use to send encrypted messages to recipients external to the department. The message can only be opened by the authorised recipient who, upon receiving the secure email, is required to use an account login and password to gain access to the email content.

The department has allowed its staff to choose whether to use the encrypted email service and has not provided them with adequate training about it. The additional security measures mean using the encrypted service takes more time than it usually takes to send a regular email. As a result, most staff do not use it.

Departmental officers at the child safety service centres we attended were not using the encrypted email service to send emails to service providers. Most were not aware that the encrypted email service was available and instead were using regular emails to exchange child safety information.

Should an unencrypted email with sensitive information about a child be sent to the wrong recipient, there are no security measures in place to stop that recipient viewing the information.

The department has advised us that it is planning to trial a new encrypted email solution that is simpler to use than the existing system and gives the sender the ability to restrict the recipient from printing, copying, saving or forwarding the email.

Cyber security controls for information systems

The department implemented cyber security controls to improve the security of its information systems, including:

- developing cyber security plans for new systems
- checking its existing systems for security weaknesses by completing penetration testing (which tests whether security can be breached), including on its main system for storing and managing child safety information—the Integrated Client Management System (ICMS)
- completing simulated hacker attacks against Internet-connected systems.

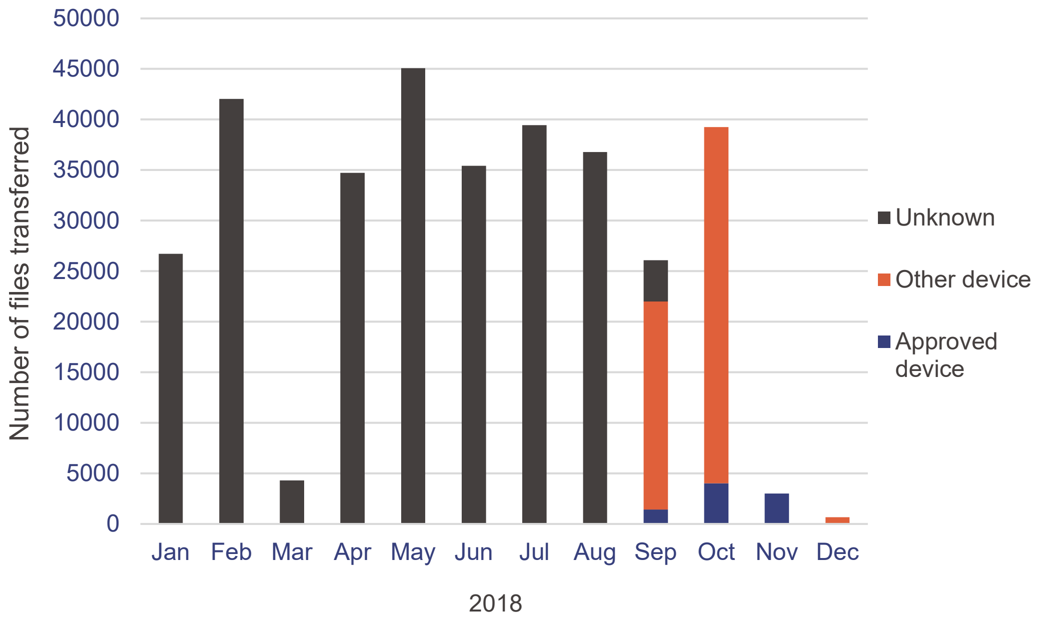
USB memory sticks

The department still allows its staff to transfer information from departmental systems onto USB memory sticks. When sensitive data is transferred onto removable media it should be encrypted to protect it from disclosure if accidentally left in a public place, lost or stolen.

The department has introduced a pop-up message that warns users who connect a USB device to their workstation to ensure it is a department-approved encrypted USB memory stick.

Figure 2A shows large numbers of files were transferred from departmental computers using a USB device in 2018. The approved USB device only accounted for 10 per cent of the files transferred between September and November 2018. Prior to September 2018, the department did not record in its use logs whether its approved encrypted USB memory stick was being used.

Figure 2A
USB use January to December 2018



Note: The department could not produce data showing the type of USB used prior to September 2018. Also, the department underwent a system upgrade between February and March 2018, which resulted in an interruption to the USB tracking service for March 2018.

Source: Queensland Audit Office, from USB use logs provided by the department.

While the department is logging these data transfer events, the logs are not actively monitored so it does not know when sensitive child safety data is copied to unprotected USB devices. This means that incidences may not be detected or managed within an appropriate timeframe, with an investigation only occurring when a complaint is received.

What still needs to be done

Information privacy and security training

The department needs to ensure its staff receive regular information privacy and security training.

Currently, departmental officers complete information privacy and security training as part of their induction into the department. There has not been any requirement for staff to complete refresher training on either topic. The department has acknowledged that it could be ‘many years’ since staff have completed the training.

In December 2018, the Office of the Information Commissioner released a report entitled *Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations*.

The report audited how three Queensland government agencies (not including the department) educated and trained their employees about information privacy and security. It recommended all agencies train and educate their employees about information privacy and security obligations and expectations as a strategy to mitigate the risk of a privacy breach. This included mandatory induction and refresher training.

While the department was not one of the agencies audited, recommendations were particularly relevant to it and other child protection agencies given the highly sensitive information they collect and manage.

The department is reviewing its induction training materials and has recently made refresher training on information privacy and security mandatory for all staff every two years.

Reviewing user access levels

To ensure the security controls remain effective, the department needs to conduct user access reviews regularly to detect and correct unnecessary information system access.

The department's main information system for recording and storing child safety information, the ICMS, has security controls that restrict access to only authorised users. It also has the ability to restrict access to individual cases. All user activities in the ICMS are recorded. Access levels for the ICMS are also used for the department's CSXpress and Carer Connect apps (which provide access to child safety officers and foster and kinship carers respectively).

The department has not regularly reviewed the access-levels of ICMS users. In fact, since our 2015 report, the only statewide user access review of ICMS was completed in January 2019, which was after we started our follow-up audit. Of the 3 130 user accounts reviewed by the department in January 2019, 314 required changes to access levels, including some that required complete removal of access to the system.

Mandatory use of secure information channels

The department still needs to improve its controls over securely exchanging child protection information.

To reduce the risk of intentional and unintentional loss, theft and/or disclosure of sensitive information, the department should mandate that its staff use secure communication channels when sending child safety information.

In the absence of any alternative secure means of exchanging information, it needs to adequately train staff in the use of the existing encrypted email service and any future solution it implements.

Security standards for service providers

We recommended that the department develop security standards for service providers. These standards should be included in service agreements.

Status: **Partially implemented**

In 2015, we found that the department's service providers needed to improve the security of their information technology environments to be in line with industry standards. While the department had formally communicated its expectations that service providers are to comply with legislation, it had not set minimum information security standards for service providers on how to protect child safety information or how to manage security risks when using outsourced services or Cloud service providers.

Security risks of non-government service providers that we identified in our 2015 audit included unauthorised access by hackers or other case workers because of inadequate password, access and internet security controls. The organisations needed to tighten controls relating to information technology administrator accounts and virus management.

Progress made

The department has taken some limited action toward implementing this recommendation. But it has not set minimum information security standards for its service providers on how child safety information should be stored, processed and transmitted.

It does specifically refer service providers to the need to comply with the *Information Privacy Act 2009* in their service agreements, but not to any information security standards.

Legal advice

In 2015, the department obtained legal advice on the privacy and confidentiality impacts of the Advice, Referrals and Case Management system (ARC). At the time, it was in the process of introducing ARC for use by non-government organisations that provide early intervention family support services. This included advice that the Information Privacy Act and confidentiality provisions in the *Child Protection Act 1999* applied to personal information collected by service providers and stored in ARC. It also concluded that the department had taken reasonable steps to safeguard personal information in ARC.

Security guidance

The department uses the Queensland Government Service Agreement standard terms for its non-government service providers. It includes clauses requiring service providers to:

- comply with Parts 1 and 3 of Chapter 2 of the Information Privacy Act, which includes compliance with the Information Privacy Principles (IPPs) set out in that Act and obligations about transferring personal information outside Australia.

  IPP 4 deals with storage and security of personal information. It states that documents containing personal information under the control of an agency must be protected against loss, unauthorised access, use, modification, or disclosure, and any other misuse. It does not give any specific guidance on how an agency is to do this
- not transfer personal information outside Australia without the department's consent
- restrict access to personal information to only those officers who need it to perform their duties
- comply with the privacy and security measures the department notifies it about from time to time.

The department advised us that it uses the standard Queensland Government Service Agreement for consistency with contracting service providers. It has been drafted by crown law and is approved for general use by government.

The department hasn't defined any minimum security standards that non-government organisations providing services on behalf of the department must meet, nor has the department issued service providers with guidance and examples of managing child safety information securely. For example, it has not defined security standards relating to the electronic storage of child safety records. However, in November 2015 the department reminded home care providers that information should not be stored overseas.

Service providers we visited during this follow-up audit told us that security requirements for electronic documents are still not clear and they need guidance on how to deal with risks, for example, when sending sensitive information by email.

The department advised us that service providers are expected to seek their own legal advice on how to comply with their service agreement.

Checking compliance with privacy and information security requirements

The department monitors service providers' compliance with information privacy and security obligations. But this monitoring is limited and does not provide a high level of assurance over the privacy and security of information.

Inspections of licensed care providers

The department conducts inspections of licensed care providers (for example, residential care facilities). Its inspections include a high-level check of the security and confidentiality of organisations' data for compliance with security and confidentiality requirements under the *Child Protection Act 1999*. The department provides a checklist to assist its staff conducting inspections but the guidance it provides is limited.

In November 2018, the department's own internal audit of licensing checks found that inspections were not occurring as frequently as required and the approach taken in issuing non-compliance findings differed by region.

In 2018, Child Safety Licensing published a range of PowerPoint-based training modules directed at staff responsible for licensing activities. These online resources have also been supported by face-to-face delivery, where possible. It is developing a series of further online modules. The department is also working to develop a risk-based assurance map, and child safety monitoring and enforcement strategy.

Audits of compliance with privacy and information security requirements

The Department of Communities, Disability Services and Seniors provides the department with the results of audits completed by trained external auditors under the Human Services Quality Framework (HSQF). All organisations funded by the department must comply with the Human Services Quality Standards, which includes performance indicators for assessing compliance. Performance Indicator 1.7 requires organisations to have:

> … effective information management systems that maintain appropriate controls of privacy and confidentiality for stakeholders.

The HSQF's user guide provides organisations with limited information about what they need to do to meet that standard. We saw little evidence in HSQF audit reports of any real focus on management and security of electronic information.

The auditors have a process for following up where the audits identify major non-conformance issues to assess whether the issues are subsequently rectified.

What still needs to be done

The department needs to develop clear minimum security standards and guidance for its service providers and reference them in service agreements.

The department should adopt a more systematic and proactive inspections and monitoring framework of service providers' compliance with the security standards. It needs to provide greater guidance to staff conducting inspections.

The department has requested the Department of Communities, Disability Services and Seniors amend the HSQF user guide to specify that organisations document and implement processes for managing the security of sensitive information relating to children and young people in care. It will also require that the implemented processes should address internal and external information technology and systems risks and identify controls for those risks.

The department also advised it intends (but has not yet started) to:

- develop a fact sheet or best practice guide for service providers on steps to identify and address information technology and systems risks and control mechanisms
- work with the Human Services Quality Framework team to develop a guidance note for auditors about assessing compliance with the changes to performance indicator 1.7, including the treatment of non-compliance with this requirement.

Appendices

A. Full responses from agency

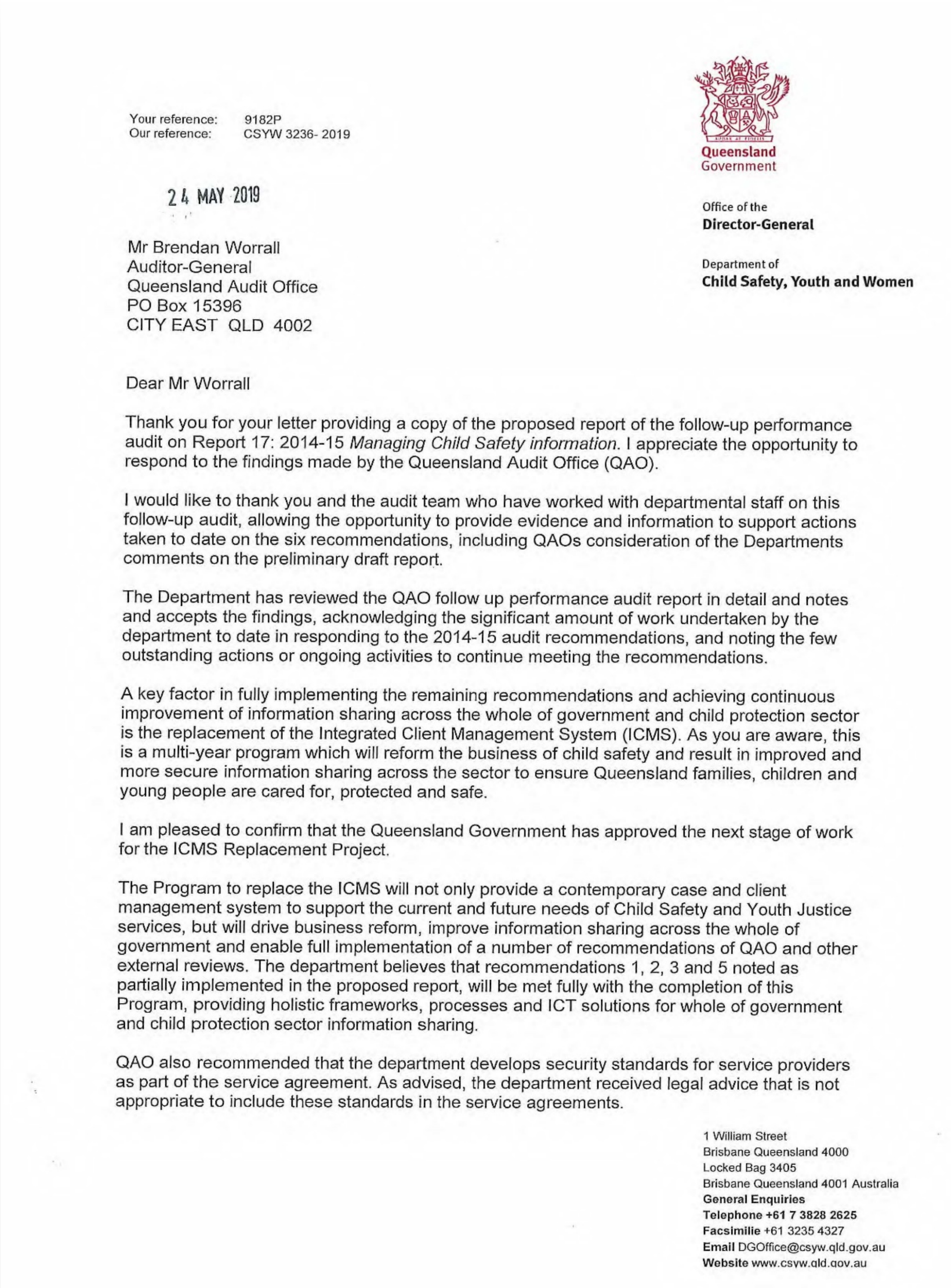
As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to the Department of Child Safety, Youth and Women.

The head of the agency is responsible for the accuracy, fairness and balance of their comments.

We also provided a copy of the report to the Department of Education for their information due to the implications of some of the recommendations on the department.

This appendix contains their responses.

Comments received from Director-General, Department of Child Safety, Youth and Women



Your reference: 9182P
Our reference: CSYW 3236- 2019

Queensland Government

Office of the
Director-General

Department of
Child Safety, Youth and Women

24 MAY 2019

Mr Brendan Worrall
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr Worrall

Thank you for your letter providing a copy of the proposed report of the follow-up performance audit on Report 17: 2014-15 *Managing Child Safety information*. I appreciate the opportunity to respond to the findings made by the Queensland Audit Office (QAO).

I would like to thank you and the audit team who have worked with departmental staff on this follow-up audit, allowing the opportunity to provide evidence and information to support actions taken to date on the six recommendations, including QAOs consideration of the Departments comments on the preliminary draft report.

The Department has reviewed the QAO follow up performance audit report in detail and notes and accepts the findings, acknowledging the significant amount of work undertaken by the department to date in responding to the 2014-15 audit recommendations, and noting the few outstanding actions or ongoing activities to continue meeting the recommendations.

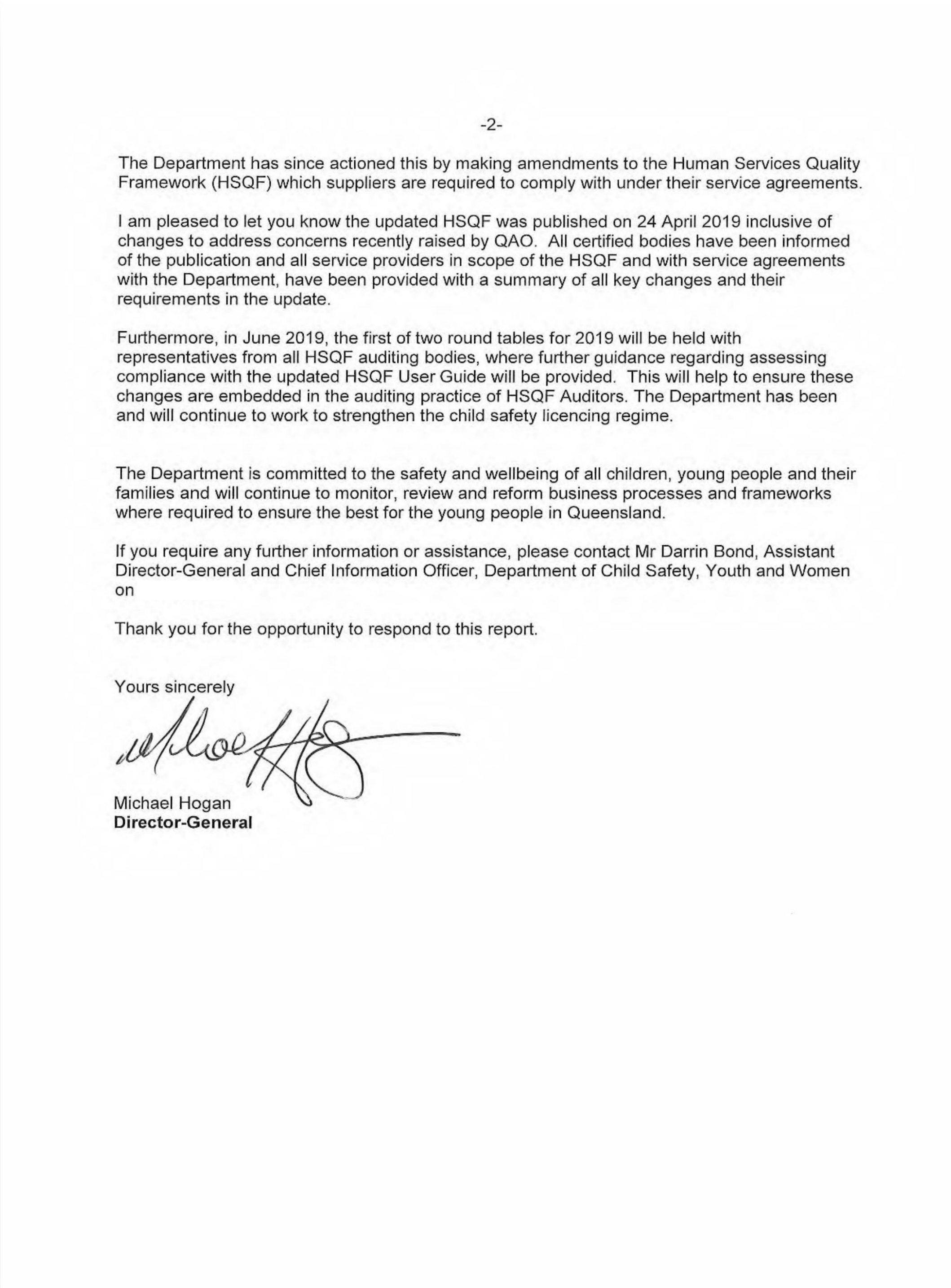
A key factor in fully implementing the remaining recommendations and achieving continuous improvement of information sharing across the whole of government and child protection sector is the replacement of the Integrated Client Management System (ICMS). As you are aware, this is a multi-year program which will reform the business of child safety and result in improved and more secure information sharing across the sector to ensure Queensland families, children and young people are cared for, protected and safe.

I am pleased to confirm that the Queensland Government has approved the next stage of work for the ICMS Replacement Project.

The Program to replace the ICMS will not only provide a contemporary case and client management system to support the current and future needs of Child Safety and Youth Justice services, but will drive business reform, improve information sharing across the whole of government and enable full implementation of a number of recommendations of QAO and other external reviews. The department believes that recommendations 1, 2, 3 and 5 noted as partially implemented in the proposed report, will be met fully with the completion of this Program, providing holistic frameworks, processes and ICT solutions for whole of government and child protection sector information sharing.

QAO also recommended that the department develops security standards for service providers as part of the service agreement. As advised, the department received legal advice that is not appropriate to include these standards in the service agreements.

1 William Street
Brisbane Queensland 4000
Locked Bag 3405
Brisbane Queensland 4001 Australia
General Enquiries
Telephone +61 7 3828 2625
Facsimilie +61 3235 4327
Email DGOffice@csyw.qld.gov.au
Website www.csyw.qld.gov.au



-2-

The Department has since actioned this by making amendments to the Human Services Quality Framework (HSQF) which suppliers are required to comply with under their service agreements.

I am pleased to let you know the updated HSQF was published on 24 April 2019 inclusive of changes to address concerns recently raised by QAO. All certified bodies have been informed of the publication and all service providers in scope of the HSQF and with service agreements with the Department, have been provided with a summary of all key changes and their requirements in the update.

Furthermore, in June 2019, the first of two round tables for 2019 will be held with representatives from all HSQF auditing bodies, where further guidance regarding assessing compliance with the updated HSQF User Guide will be provided. This will help to ensure these changes are embedded in the auditing practice of HSQF Auditors. The Department has been and will continue to work to strengthen the child safety licencing regime.

The Department is committed to the safety and wellbeing of all children, young people and their families and will continue to monitor, review and reform business processes and frameworks where required to ensure the best for the young people in Queensland.

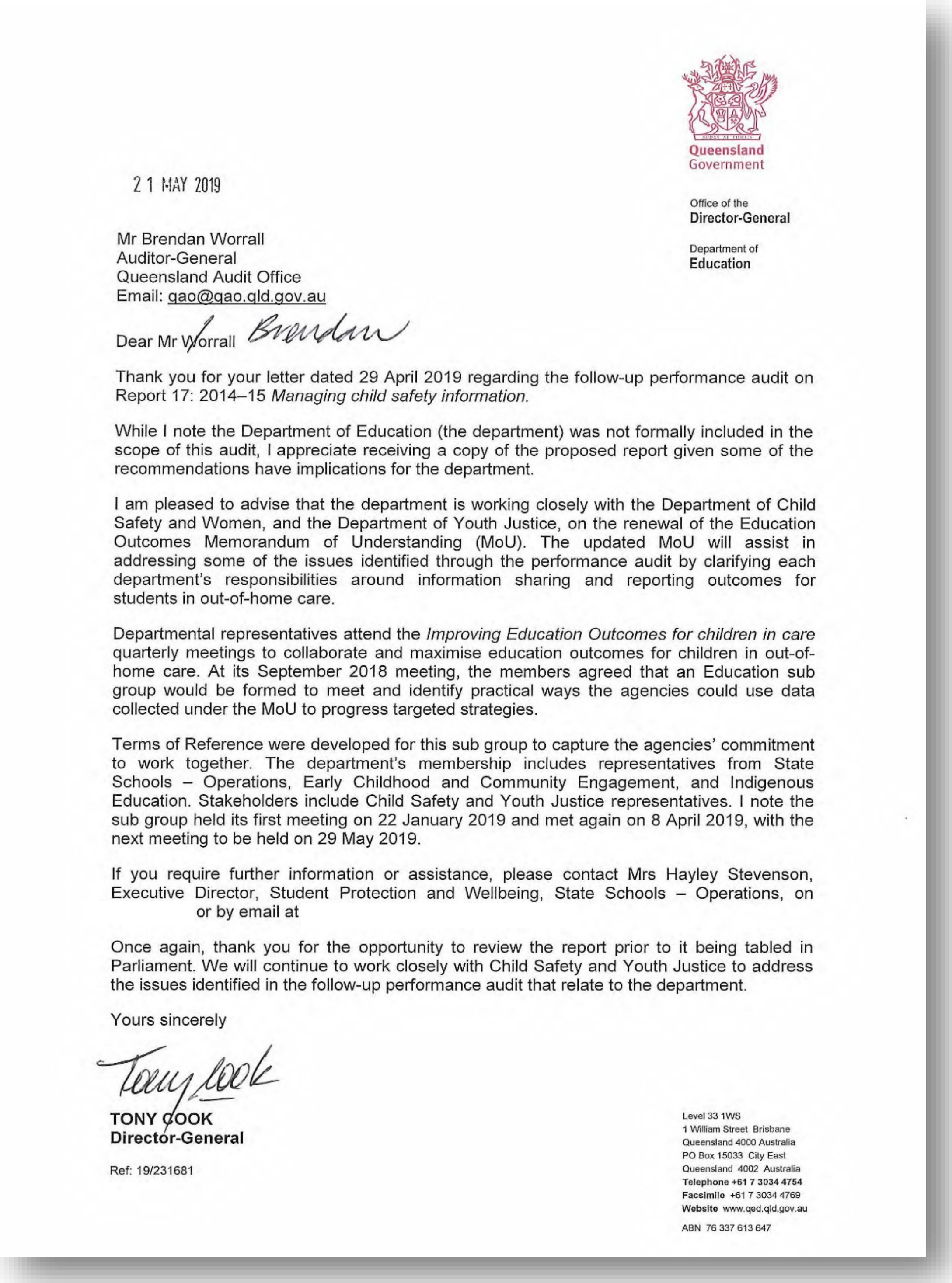
If you require any further information or assistance, please contact Mr Darrin Bond, Assistant Director-General and Chief Information Officer, Department of Child Safety, Youth and Women on

Thank you for the opportunity to respond to this report.

Yours sincerely

Michael Hogan
Director-General

Comments received from Director-General, Department of Education



Queensland
Government

Office of the
Director-General

Department of
Education

21 MAY 2019

Mr Brendan Worrall
Auditor-General
Queensland Audit Office
Email: qao@qao.qld.gov.au

Dear Mr ~~Worrall~~ Brendan

Thank you for your letter dated 29 April 2019 regarding the follow-up performance audit on Report 17: 2014–15 *Managing child safety information.*

While I note the Department of Education (the department) was not formally included in the scope of this audit, I appreciate receiving a copy of the proposed report given some of the recommendations have implications for the department.

I am pleased to advise that the department is working closely with the Department of Child Safety and Women, and the Department of Youth Justice, on the renewal of the Education Outcomes Memorandum of Understanding (MoU). The updated MoU will assist in addressing some of the issues identified through the performance audit by clarifying each department's responsibilities around information sharing and reporting outcomes for students in out-of-home care.

Departmental representatives attend the *Improving Education Outcomes for children in care* quarterly meetings to collaborate and maximise education outcomes for children in out-of-home care. At its September 2018 meeting, the members agreed that an Education sub group would be formed to meet and identify practical ways the agencies could use data collected under the MoU to progress targeted strategies.

Terms of Reference were developed for this sub group to capture the agencies' commitment to work together. The department's membership includes representatives from State Schools – Operations, Early Childhood and Community Engagement, and Indigenous Education. Stakeholders include Child Safety and Youth Justice representatives. I note the sub group held its first meeting on 22 January 2019 and met again on 8 April 2019, with the next meeting to be held on 29 May 2019.

If you require further information or assistance, please contact Mrs Hayley Stevenson, Executive Director, Student Protection and Wellbeing, State Schools – Operations, on or by email at

Once again, thank you for the opportunity to review the report prior to it being tabled in Parliament. We will continue to work closely with Child Safety and Youth Justice to address the issues identified in the follow-up performance audit that relate to the department.

Yours sincerely

Tony Cook

TONY COOK
Director-General

Ref: 19/231681

Level 33 1WS
1 William Street Brisbane
Queensland 4000 Australia
PO Box 15033 City East
Queensland 4002 Australia
Telephone +61 7 3034 4754
Facsimile +61 7 3034 4769
Website www.qed.qld.gov.au
ABN 76 337 613 647

B. Audit objectives and methods

The objective of the audit was to assess whether the Department of Child Safety, Youth and Women (the department) has effectively implemented the recommendations we made in *Managing child safety information* (Report 17: 2014–15).

The audit addressed the objective through the following criteria as set out in figure B1.

Figure B1
Audit criteria

Criteria		Sub-criteria	
1	The department has actioned the recommendations	1.1	The department has implemented the recommendations in accordance with its response or has taken appropriate alternative actions
		1.2	The department has implemented the recommendations in a timely manner
2	The department has addressed the underlying issues which led to the recommendations	2.1	The department has addressed the issues that led to the recommendations
		2.2	The department's actions have resulted in improvements in its management and sharing of child safety information with other government agencies and with child safety service providers

Source: Queensland Audit Office.

Entity subject to this audit

We audited the Department of Child Safety, Youth and Women.

We also engaged with the Department of Education, the Department of Health, the Queensland Police Service, and some non-government organisations funded by the department to provide family support and child protection services.

Audit approach

The audit was conducted between October 2018 and March 2019. The audit included:

- a self-assessment by the department of its progress in implementing our recommendations
- interviews with the department officers
- interviews with officers of non-government service providers
- documentation review, including analysis of service agreements, policies, guidelines, and manuals.

Performance engagement

This audit has been performed in accordance with the Standard on Assurance Engagements ASAE 3500 *Performance Engagements,* issued by the Auditing and Assurance Standards Board. This standard establishes mandatory requirements, and provides explanatory guidance, for undertaking and reporting on performance engagements.

The conclusions in our report provide reasonable assurance that the objectives of our audit have been achieved. Our objectives and criteria are set out in Figure B1 above.

We assessed whether each recommendation has been fully implemented, partially implemented, not implemented, or is no longer applicable. Figure B2 provides the definition we use for each status.

Figure B2
Definitions of implementation status

Status	Definition
Fully implemented	Recommendation has been implemented or alternative action has been taken that addresses the underlying issues identified and no further action is required. Any further actions are business as usual.
Partially implemented	Significant progress has been made in implementing the recommendation or taking alternative action; however, further work is required before it can be considered business as usual. This also includes where the action taken was less extensive than recommended, as it only addressed some of the underlying issues that led to the recommendation.
Not implemented	No or minimal actions have been taken to implement the recommendation or the action taken does not address the underlying issues that led to the recommendation. This also includes where government or the agency did not accept the recommendation.
No longer applicable	Circumstances have fundamentally changed, making the recommendation no longer applicable. For example, a change in government policy or program has rendered the recommendation no longer relevant.

Source: Queensland Audit Office.

C. Report 17: 2014–15 recommendations

We made six recommendations to the Department of Child Safety, Youth and Women in *Managing child safety information* (Report 17: 2014–15).

Figure C1
Recommendations made in Report 17: 2014

	Recommendations
1	Develops and implements a coordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain.
2	Implements contemporary information systems that: • integrate the information that is held across all parts of child safety services • automate information exchange with authorised persons • are flexible and adaptable to changes in business processes • provide relevant functionality and reporting • enable the collection of relevant information and promote outcomes-based reporting • make it easier to manage multiple records on the same client within different media and in different formats.
3	Uses information available across organisational boundaries within the service chain to gain insights and improve service outcomes. For example, to: • verify whether children not recorded as attending schools are really not attending schools and implement plans for their educational support • implement effective measures to address school attendance, suspension, exclusions, absences and abscondments to evaluate the success of its partnership with Department of Education • monitor all aspects of child safety services including those where the responsibility is devolved to other government departments • establish regular monitoring processes for education support plans, health passports and transition plans • implement mandatory recording of reference keys for the Integrated Client Management System and OneSchool to ensure that information on the same child is being recorded correctly and consistently in the two systems • implement measures to improve and monitor the completion and timeliness of information about transition arrangements within the case plans and transition from care plans.
4	Specifies the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system.

	Recommendations
5	Improves security within the existing environment by: • extending secure email services in the current system to encrypt information exchange with all service providers • identifying where sensitive child safety information is stored in the file system and ensuring access controls are authorised by business owners • reviewing and updating user access levels regularly for key child safety systems • preventing transfer of sensitive child safety data from the departmental network to unencrypted, removable media (such as USB memory sticks).
6	Develops security standards for service providers. These standards should be included in service agreements.

Source: Queensland Audit Office.

Auditor-General reports to parliament

Reports tabled in 2018–19

1. Monitoring and managing ICT projects
   Tabled July 2018
2. Access to the National Disability Insurance Scheme for people with impaired decision-making capacity
   Tabled September 2018
3. Delivering shared corporate services in Queensland
   Tabled September 2018
4. Managing transfers in pharmacy ownership
   Tabled September 2018
5. Follow-up of Bushfire prevention and preparedness
   Tabled October 2018
6. Delivering coronial services
   Tabled October 2018
7. Conserving threatened species
   Tabled November 2018
8. Water: 2017–18 results of financial audits
   Tabled November 2018
9. Energy: 2017–18 results of financial audits
   Tabled November 2018
10. Digitising public hospitals
    Tabled December 2018
11. Transport: 2017–18 results of financial audits
    Tabled December 2018
12. Market-led proposals
    Tabled December 2018
13. Health: 2017–18 results of financial audits
    Tabled February 2019
14. Queensland state government: 2017–18 results of financial audits
    Tabled February 2019
15. Follow-up of Oversight of recurrent grants to non-state schools
    Tabled March 2019
16. Follow-up of Maintenance of public schools
    Tabled April 2019
17. Managing consumer food safety in Queensland
    Tabled May 2019
18. Local government: 2017–18 results of financial audits
    Tabled May 2019
19. Education: 2017–18 results of financial audits
    Tabled May 2019
20. Follow-up of Managing child safety information
    Tabled May 2019

Audit and report cost

This audit and report cost $162 000 to produce.

Copyright

ISSN 1834-1128.

qao.qld.gov.au/reports-resources/parliament

Suggest a performance audit topic

Contribute to a performance audit in progress

Subscribe to news

Connect with QAO on LinkedIn

T: (07) 3149 6000
M: qao@qao.qld.gov.au
W: qao.qld.gov.au
53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Queensland Audit Office
Better public services