SENTRAL EDUCATION

Sydney +61 2 9029 3993
Melbourne +61 3 9005 5304
Brisbane +61 7 3102 2576
Adelaide +61 8 7200 3703
Perth +61 8 6102 3638

Suite 19, 265-271 Pennant Hills Road,
Thornleigh NSW 2120
Mailing address P.O. Box 4401,
Thornleigh NSW 2120
Fax 02 8209 4948
ABN 24 085 316 310

www.sentral.com.au

Official Statement Regarding Information Risk of the Sentral Solution

This documentation has been provided in response to request for information to schools relating to *Appendix 1: Questions to consider while assessing the information risk of Student Reports solutions* as issued by the Department of Education in Victoria, and relates to the use of the Sentral school information system (including its Reports functionality) within schools.

1. Inter-operability with School systems

The reports and outputs from the application or service should be easily transferred onto Department systems

a. Can reports from the application or service be easily exported from / imported into CASES 21?

Yes. Sentral feeds information from CASES21 to provide its baseline data. From June 2015, Sentral will use the EduHub service offered by the Department to automate this process. Sentral also offers exports of data back INTO CASES21 for Attendance and AusVELS Reporting data.

2. Disaster Recovery

Will the service provider services be impacted by a disaster or outage?

a. Does the service provider have capability to restore the services in the event of a disaster / disruption at the service provider facility?

Yes. Sentral is typically housed on school equipment, so there is no central point of failure as with some hosted options. In the event of an outage affecting your Internet connectivity, the service remains available for use within school. In the event of a disaster, disruption or failure of your Sentral server, we can provide a temporary, remote hosting facility to ensure continuity of service.

b. Does the service provider offer Service Level Agreements (SLAs) for the service?

Yes. Sentral provides a range of SLA options to suit individual school needs and budgets.

c. Does the service provider have an up-to-date Disaster Recovery Plan that was tested successfully within the past 12 months?

Yes. The process for restoring a school's data in the event of a failure of local equipment is documented and tested quarterly (minimum). It is important to note that Sentral Education takes no responsibility for local school equipment and/or failures as these are the responsibility of the school and/or the school's hardware vendor. Schools should ensure that their server equipment is appropriately maintained and covered by vendor warranty and adequate support arrangements.

3. Privacy of Information

Schools moving to a cloud delivery model need to ensure that they can meet their obligations under Victorian privacy laws.

> ***It is important to understand that while Sentral does offer cloud-based solutions, most schools will opt to host Sentral locally on their school premises. As such, many of the security/privacy concerns affecting cloud-based solutions are not present with Sentral.***
>
> ***This means that all your school data remains ON SCHOOL PREMISES.***

a. Will information be stored and/or processed in Australia?
Yes. Your information remains solely on your school site, it remains confidential and is treated as such at all times.

b. Does the service require access to the application or service from parties overseas, such as by developers? If so, please detail specifics.
No. All Sentral Education staff with the potential capacity to access school data are permanent employees based in Australia. They have all undergone relevant background/working with children checks and are bound by confidentiality agreements to protect school and student data.

c. Will the Department be able to access, modify and retrieve all stored information (including personal information) for modification and reporting purposes?
Yes. Sentral Education has a long history of collaboration with various state Departments and other agencies/jurisdictions. We will comply with any requests for information from the Department, court orders or Police investigations. In all cases we will require the approval of the school Principal unless otherwise required due to legal reasons.

d. Will individuals be able to request access, amendments or deletion of the information? If so please provide details about how they can do this.
System and role based access permissions within Sentral control who can access, amend or delete data. The Principal is responsible for managing these permissions or delegating them to another appropriate individual.

Sentral maintains comprehensive access and audit logs which can be used to track access and modification of data and configurations in the event of misuse. Regular backups also allow tracing of the complete system state over a period of days, weeks and months.

4. Security Incident Management

THIS IS A HIGH RISK QUESTION; SCHOOLS ARE RECOMMENDED NOT TO PROCEED IF THE SERVICE PROVIDER DOES NOT POSITIVELY RESPOND TO THIS QUESTION.

Security incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events

a. Will the Department and schools be informed of actual or suspected security incidents or data breaches?

Yes. As a locally hosted solution, by default, individuals based outside of the school cannot access the solution. Where external access has been configured, this is done **solely** through a HTTPS (secure) connection allowing only web-based access to the system. In addition only the modules enabled by the school administrator are made available externally. This greatly reduces the risk of unauthorised access to the system by allowing only essential functions and data to be viewed outside the school's local network.

In the event of a security incident that affects schools, Sentral will notify all current users of the system. To date we have an exemplary record on security with no known system-level breaches across 10 years in more than 1,500 sites.

Schools may experience local security breaches eg a student who uses a teachers access credentials. In such cases, once notified by the school, Sentral Education will use inbuilt audit logs to identify the actions of that user.

a. Does the service provider have a process for managing security incidents?

Yes. Security-related incidents are treated with the utmost priority and internal processes require them to be raised immediately to the relevant manager for further analysis and remediation. We are committed to a full disclosure policy relating to any incidents that might occur.

b. Will access security logs be kept during the contract period by the service provider?

Yes. Audit logs relating to access to the solution are kept indefinitely while the system is actively used by a school. Detailed access logs (down to an individual page/request) are kept for a period of 1 month by default.

5. Review

When necessary the Department and school should be able to review the service provider systems

a. Will the service provider sign a contract that allows the Department or school to regularly review and/or conduct investigations on the service provider and on its systems to ensure that the controls and capabilities are in place?

Yes. It should be noted that, as most of the solution is hosted on school-premises in most cases, many of the obligations/requirements are outside of our control.

6. Information Security Policies and controls at the service provider

The school should ensure that the service provider has the capability and processes to safeguard information

a. Does the service provider have policies on information, ICT, personnel and physical security?

Yes. Sentral Education has a comprehensive suite of policies to guide staff behaviour. All staff undergo thorough background checks and are required to hold the relevant working with children checks or equivalent for their jurisdiction.

b. Are the service provider's staff security responsibilities and obligations documented and communicated?

Yes. Security and confidentiality are taken very seriously and all staff are regularly reminded of their obligations regarding handling of confidential data. All office space that may house confidential data is protected by access-controlled doors secured by swipe card. All print copies are shredded when they are no longer required.

c. Does the service provider train their staff regarding security obligations and good security practices?

Yes. New staff are trained on security handling obligations and best practices during their induction. Staff meetings regularly review security practices and handling of sensitive information. Policies are reviewed with staff annually.

d. Does the service provider conduct
i. Regular software and system patch management
ii. Security event management
iii. Antivirus, malware and vulnerability management
iv. Record and manage logs of systems and alert on security incidents

Yes. Sentral Education performs regular monitoring and testing of our standard production image and will deploy security fixes and software updates automatically to schools.

Security logs are monitored and automatically report suspicious activity back to a centralised monitoring solution.

Schools are expected to maintain good security practices on their local network and notify us if there are any issues that may impact on the operation of the Sentral system.

e. Has the service provider's cloud environment been certified against recognised security standards (e.g. ISO 2700x, PSPF) by an independent and qualified auditor?

For local school deployments, this is not applicable as the environment is the responsibility of the school. Where a school has opted for a cloud-based deployment, the environment undergoes a range of auditing and accreditation. Full details of this can be found online at: http://aws.amazon.com/compliance/

7. Accessibility

Can the service be used by people with physical disabilities?

a. Is the service WCAG 2.0 compliant?

Yes. Sentral is WCAG 2.0 Level AA complaint.

8. Employing the right people

The service provider should ensure that staff members are screened they are engaged

a. Does the service provider do pre-employment or pre-contract screening and background checks before engaging their staff?

Yes. All staff are residents of Australia and undergo relevant background checks and *Working With Children Checks* (or equivalent for their jurisdiction) before they commence employment. We voluntarily provide this higher level of clearance even though our staff do not have unsupervised contact with children.

b. Are staff monitored on a regular basis to ensure their ongoing eligibility to access information?

Yes. All checks are kept current and staff are required to maintain current *Working with Children Checks*. Any staff who may fail to meet the requirements for employment are removed from any position that provides access to data while an investigation is undertaken.

9. Physical security

Physical security at service provider locations that store the Department's information

a. Are physical security controls in place at all locations of the service provider where Departmental information is held?

Physical security controls are the responsibility of the school, as the information typically resides on school premises. Physical door access controls, as well as after hours alarm system, protect any information that may be temporarily held within the Sentral offices.

b. Are physical security controls in place around the transfer, storage and disposal of Departmental information?

All Departmental information physically resides with the school and remains their responsibility.

c. Does the service provider undertake regular compliance assessments against Australian or international security standards (e.g. PSPF, ISO2700x)?

Compliance assessments against ISO27001 and other standards are undertaken for any cloud-based components of the Sentral solution. Local school-based information resides within the school's environment.

10. Security of the service or application

Technical security of the service or application provided by the service provider

a. **Does the system/service/product employ appropriate security authentication and access control mechanisms?** ***(Passwords, authorisation to selected information etc.)***

Yes. Sentral employs a flexible authentication and access control system, allowing all user management and accounts to be managed in-system, or linked to an external source such as Active Directory, Google Apps or a corporate Department portal (if it supports SAML).

b. Does the application undergo detailed security testing prior to use in production?

Yes. All software developed by Sentral Education undergoes a range of processes designed to ensure security, including but not limited to:

- Training of staff on secure programming principles
- Defensive programming styles to mitigate common vulnerabilities
- Peer code review
- Unit and functional testing
- Periodic penetration testing

11. Completion of contract

Questions to consider when the contract ends.

a. On cessation of the contract, does the service provider provide a mechanism to transfer all information back to the school for archival and record keeping purposes, and destroy or permanently de-identify information kept by this 3rd party?

Yes. In the event of a termination or un-renewed contract, a school can request an export of core data in an application neutral format (usually a series of CSV and attachment data files) for a small handling fee.

b. Does the contract allow school to switch to another service provider should the contracted services prove unsatisfactory?

Yes. Sentral does not use lock-in contracts and schools only need to make a 12 month commitment. At the end of the 12 month period it is each school's decision to renew the software licence; however should they choose not to do so, the software will cease to function and must be removed from their systems.

Should you have any further questions or concerns, please do not hesitate to contact:

Dan Wheaton
Infrastructure Manager
dan.wheaton@sentral.com.au