i·DAT®
International Diagnostic & Admissions Test

+61 2 8316 6633

Level 1, 338 Pitt Street
Sydney NSW 2000

www.idat.org
info@idat.org

Basic Information to IDAT Partners for data storage and protection:

- Cloud based data centre: Amazon Web Services
- Geographic Location: IDAT uses two major nodes. Asia: Singapore
  Europe: Frankfurt, Germany
- Schools may specify their preferred AWS hosting cloud location from above. Should they wish to use another AWS location, it may be available at a price.
- IDAT has a full Disaster Recovery and Business Continuity Plan in regard to data storage and test sites. This includes back up operations.
- IDAT has a Data Loss Prevention solution in place through Amazon Web Services.
- IDAT does not encrypt customer fata on disk/storage within our company.
- IDAT maintains logs for 365 days.
- IDAT supports secure deletion of archived data as determined by customers and has controls in place to prevent leakage or intentional compromise between customers.
- Only schools have access to their own data and information in their school portal for IDAT Concise testing. Only schools have access to their own IDAT Concise portal. If there are emergencies, or issues, this data can be accessed or viewed by IDAT with school permission.
- Students log in to take the tests using a test code. They cannot log in anonymously, and each school can only their own student data.
- All access to IDAT, its portal, testing and other information is via web browser.
- The IDAT Concise portal gathers information such as student name, gender and date of birth. Only schools have access to this data with personal information.
- Information for data analysis of correct questions by type may be gathered by IDAT. Personal student data (names and DOB) are in school portal only. The IDAT research team will use student gender, replies to questions and geographical regions to review test effectiveness. You can be notified upon request. No personal student data is used for this.
- IDAT uses multi-factor Identity Management solutions to protect its infrastructure and customer data.
- IDAT has technical control capabilities to enforce customer data retention.
- The IDAT IT management is liable for any breaches or unapproved exposure of data.
- Data migration does not occur unless there are abnormal circumstances. If data migration is required, customers would be provided with documentation that describes what is occurring with their data and approval will be sought.
- Customers are notified via email to their registered contact address of any material changes to our information security and/or privacy policies.
- Amazon Web Services provides virtual machine management infrastructure include a tamper audit to detect changes.
- Customers are provided with capabilities to restore virtual machines to previous states in time if required.
- All documents relating to internet security, policies, non-disclosure or confidentiality agreements and data protection are reviewed annually.
- IF required, IDAT can provide customers with the procedure for exiting a service agreement, including assurance to sanitize al data related to that customer when they have exited the IDAT portal.

IDAT & GDPR Compliance

1. Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved.
2. IDAT processes children's personal data with emphasis on protecting them from the outset, and have design our systems and processes with this in mind.
3. Compliance with the data protection principles and in particular fairness is central to all IDAT's processing of children's personal data.
4. For the **full IDAT tes**t, IDAT has a lawful basis for processing a child's personal data. Consent is required by the parent and child. IDAT realized that in the UK only children aged 13 or over are able provide their own consent. However IDAT seeks parental consent and child consent for all applicants.
5. For the **IDAT Concise**, only the school has access to student data for their own school. No other customer may access this data.
6. For **IDAT Concise** portal emergencies or issues with the system, IDAT may upon request of the school, access student data for troubleshooting reasons.
7. IDAT recognizes children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
8. For the **full IDAT test,** IDAT endeavors to write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
9. For the IDAT Concise test, as only the school has access to student information, it is up to the school to inform students of their privacy rights and notices.
10. IDAT recognizes that children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
11. IDAT recognizes a parent or child's individual right to erasure is particularly relevant if they gave their consent to processing when they were a child.
12. IDAT uses Data Protection Impact Assessments to assess and mitigate risks to children. IDAT also considers children's, guardians and parents' point of view when designing processes.
13. IDAT regularly reviews available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.

14. IDAT does not use student's test result pages for purposes of marketing without explicit consent from children, parents and involved schools. When used for marketing, it is only ever shared with admissions and school professionals and not with the public. Student's private information is always blocked or redacted before sharing.

15. IDAT complies with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).
16. IDAT follow the approach in the Information Commissioner's Office's Data Sharing Code of Practice.

17. IDAT explains to children why the test requires the personal data we have asked for, and what we will do with it, in a way which they can understand.

18. As a matter of good practice, IDAT explains the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

IDAT Disaster Recovery Plan

The major goals of the IDAT disaster recovery plan are;

- To minimize interruptions to the normal operations, testing ,booking and communication with students and parents.
- To limit the extent of disruption and damage to data, security breaches and communications.
- To minimize the economic impact of the interruption to IDAT and its partners.
- To establish alternative means of operation of the test and its procedures in advance.
- To train IT and other personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

A complete list of Data Processing personnel and systems IT specialists is kept by the IT Manager. Please contact the IT manager for this list, should it be required by an external source. For privacy reasons, it is not in this document.

Recovery Plan Steps:

1. Assess and contain the damage.

The head of IT at IDAT will be in tight communication about what happened and how to proceed in fixing the data security breach.

The disaster recovery or business continuity plan will be enacted, along with documentation of passwords and backup of all systems.

The IT manager and damage control team needs to decide:

1. Is the breach contained?
2. How severe is the damage?
3. What steps do we need to take now?
4. Who needs to know? If sensitive data was exposed, you're likely legally required to notify those who are potentially impacted and/or government agencies.
5. How can we prevent this from happening in the future?

3. Take data restoration steps.

Every situation is unique. Some actions need to be taken immediately, while others may happen over the coming days, weeks, and months. Depending on what happened, restoration from a data security breach could mean:

- Restoring files from backup
- Changing all passwords
- Taking a system offline until security updates can be applied.
- Paying the ransom on the ransomware (which is a terrible idea, for so many reasons!)

4. Communicate.

IDAT is committed to communicating and data or security breached. First to employee, the Academic Integrity Council, and then to anyone (schools & students) affected outside your organization, IDAT will communicate

- What happened
- How you're fixing the issue.
- Any steps those impacted need to do to protect themselves.

5. Get committed to data security.

Microsoft 365 is used for:

- Identity & access management
- Threat protection
- Information protection
- Security management
- Device and application management

We also believe strongly in user data security training.

Beyond user training, IDAT safeguards using the following:

- Multi-factor authentication
- Leaked credential reporting and monitoring

- Computer firewalls
- Routine backup and recovery procedures
- Regularly applying security updates

Application & Online profile –

- for each incident an application profile must be completed and stored for future reference. The following is a list of or major application or Portals which are checked weekly and assessed for issues.
-

Application or Portal Name	Critical Y/N	Fixed Asses Y/N	Manufacturer or Provider	Comment
IDAT website			Hosted by Amazon Webservices	
IDAT Concise School Portal			IDAT IP – Hosted by Amazon Webservices	
IDAT Concise - student Test portal			IDAT IP – Hosted by Amazon Webservices	
IDAT full test portal			IDAT IP – IDAT – Hosted By Alibaba webservices	
IDAT 360 chat function			Hosted by: Zolo	
IDAT website chat function			Hosted by: Zolo	
IDAT emails server			Hosted By by Microsoft 365	
IDAT 360 video interface			Hosted by Tencent	

Inventory profile –

The inventory profile and list are updated every 6 months. We have a limited staff and the list of staff and the computers they use is confidential for the purposes of this report.
The list includes: Processing units, system printers, cameras & microphones, I/O processorss, spare displays and hard drives.
Please ask the IT Manager if you have any questions or would like access to this list/report.

Information Services Backup Procedures.

- The IT manager backs up all information daily.
- Daily saving of changed objects in the IDAT Portal and IDAT Concsie portal is conducted by the IT Manager
- The IT manager keeps a journal of all back up activities and this journal is also saved and backed up.
- On Fridays at 3 pm, AEST a complete save of all systems if done.
- All save media is stored in the Amazon Web services cloud and backed up

As part of company policy all personal computers must be backed up. Copies of the personal computer files should be uploaded to cloud storage used by IDAT.

Disaster Action Checklist

This checklist provides possible initial actions that you might take following a disaster.

1. Plan initiation:
    a. Notify senior management
    b. Contact and set up disaster recovery team
    c. Determine degree of disaster
    d. Implement proper application recovery plan dependent on extent of disaster
    e. Monitor progress
    f. Contact backup site and establish schedules
    g. Contact all other necessary personnel–both user and data processing
    h. Contact vendors–both hardware and software
    i. Notify users of the disruption of service

2. Follow-up checklist for remote work:

    a. List teams and tasks of each
    b. As IDAT uses a cloud based server, for emergency if the physical location of the IDAT IT team is compromised, they would work from home.
    c. List all personnel and their telephone numbers
    d. Establish user participation plan
    e. Set up the delivery and the receipt of mail,
    f. Establish emergency home office supplies.
    g. Rent or purchase equipment, as needed
    h. Determine applications to be run and in what sequence.
    i. Check out any off-line equipment needs for each application.
    j. Check on forms needed for each application.
    k. Check all data being taken to or used at home offices.
    l. Set up primary vendors for assistance with problems incurred during emergency.
    m. Plan for transportation of any additional items needed for home offices.
    n. Take copies of system and operational documentation and procedural manuals.

o. Ensure that all personnel involved know their tasks.
p. Notify insurance companies

Consider these recovery startup procedures for use after actual disaster.

1. The IT Manager would need to notify the CEO and Directors of IDAT. The CEO would notify the Academic Integrity Council who would handle PR and communications.
2. If required, external help of SOPHOS (IT specialist data company in UK) would be contracted to assist with data recovery and start up procedures.

Restoring the System

The IT Manager would be responsible to review the system and restore as required. Using backed up files, as noted above. The entire system may need to move servers or platforms if the current one is corrupted.

The RTO (Recovery Time Objective) for all systems for the IDAT test is 24 hours. The RTO for emails and communication is 3 hours.

The RPO (Recovery Point Objective) is 24 hours worth of data for testing or test information.

Reviewing and Testing the Disaster Discovery plan

The IT Manager has a an assistant manager trained and prepared to step in. Members of the IT team are cross-trained people so that they pivot and take on additional roles or responsibility in case someone else is not available.

The Disaster Recovery system is regularly tested (bi-monthly). Testing looks for flaws in rthe plan and keeps the plan at the top of the team's mind.

The plan is kept current, and the IT Manager records of changes to IDAT configuration, portals, applications, and backup schedules and procedures.

2. Assess and contain the damage.

The head of IT at IDAT will be in tight communication about what happened and how to proceed in fixing the data security breach.

The disaster recovery or business continuity plan will be enacted, along with documentation of passwords and backup of all systems.

The IT manager and damage control team needs to decide:

6. Is the breach contained?
7. How severe is the damage?

8. What steps do we need to take now?
9. Who needs to know? If sensitive data was exposed, you're likely legally required to notify those who are potentially impacted and/or government agencies.
10. How can we prevent this from happening in the future?

3. Take data restoration steps.

Every situation is unique. Some actions need to be taken immediately, while others may happen over the coming days, weeks, and months. Depending on what happened, restoration from a data security breach could mean:

- Restoring files from backup
- Changing all passwords
- Taking a system offline until security updates can be applied.
- Paying the ransom on the ransomware (which is a terrible idea, for so many reasons!)

4. Communicate.

IDAT is committed to communicating and data or security breached. First to employee, the Academic Integrity Council, and then to anyone (schools & students) affected outside your organization, IDAT will communicate

- What happened
- How you're fixing the issue.
- Any steps those impacted need to do to protect themselves.

5. Get committed to data security.

Microsoft 365 is used for:

- Identity & access management
- Threat protection
- Information protection
- Security management
- Device and application management

We also believe strongly in user data security training.

Beyond user training, IDAT safeguards using the following:

- Multi-factor authentication
- Leaked credential reporting and monitoring
- Computer firewalls
- Routine backup and recovery procedures
- Regularly applying security updates