2021

IT security policy

VERSION 1

TRACY PEERS

ST DAVIDS HIGH SCHOOL

IT Security Policy

The following IT security policy is designed for use in St David's High School. A failure to secure the IT systems would jeopardise the ability of a learner to the fulfilment of his or her academic potential in addition to the development of an individual able to play his or her part in society.

Whilst an IT security policy is a living document, the overall objectives remain the preservation of confidentiality, integrity, and availability of systems and information used by stakeholders of St David's High School

Standards

The policy has been developed to be consistent with industry standards such as ISO 27001, which is designed to ensure the selection of adequate and proportionate security controls. Whilst IT department acknowledge ISO 27001 as a basis for the policy development, the move towards an externally measured standard is in a stage of development rather than maturity.

Acceptable usage

Before an employee is granted access to IT systems, the relevant employment procedures must be completed. Access to restricted and confidential data

When a new user begins employment, they must read and complete the School's acceptable usage agreement. Once the user has accepted these conditions, HR will keep a record and authorised access to various IT systems.

IT Access summary

All users of IT systems and equipment require a unique identifying account (Windows Log-in) with password details only known to themselves.

Subsequent IT systems access may require further usernames or passwords which should be treated in the same manner.

Under no circumstances should any IT account details be written down unless with the prior approval of a senior leadership member.

Any additional system access must be requested via the IT Service Desk, approval will be required from the designated line manager.

All users must ensure any PC or Laptop in use is locked or logged out while unattended.

Computer screens will be locked after 10 minutes of inactivity for class rooms (Windows 10 and above) and 60 minutes for a secured office and require a password to resume.

Users are required to inform IT Service Desk of any threat and/or concerns regarding the IT systems or hardware they use as soon as possible.

Any activity on St David's High School systems or equipment may be logged by IT and used by for auditing purpose if required.

All users must read and understand the associated ICT Policies before using that technology.

Physical security and building access control

Whilst the site management team will secure the physical building security for outside working hours with the use of external locks and appropriate intrusion alarm system. Access control mechanisms such as ID Cards are fitted to selected internal doors. Additional access fobs may be utilised for to secure sensitive areas such as finance or provide rapid access for first aid purposes.

CCTV camera system provide adequate coverage to safeguard learners, assets including the access to the principle communications room.

Protection from other sources of damage such as fire or flood should be considered where appropriate in line with various risk assessments and agreed standards.

Guest access

Guest and visitor access should be administered by an inventory system, whereby all visitors should display an identifiable badge along with their name.

Additional documentation

All equipment should be listed on an inventory, please see below for a detailed breakdown.

- IT Inventory <attached PDF version> / link to web-based system. (snipe)

Data storage

Where possible, no data should be stored on computer local hard drives and should instead be stored on network files servers. Additional precautions such as un-interrupted Power Supply (UPS) should be utilised to reduce the risk of data corruption on critical systems outside the main server room.

Communications room / server room

As stated earlier, appropriate CCTV coverage must be provided in addition to multiple locks such as limited sets of key variants in addition to pin or Biometric access. The principle of least privilege should be applied.

The room(s) should not be used for additional storage, whilst an appropriate level of resilience should be provided in relation to power and temperature regulated environment. Additional considerations should also be made as the County Council share and provide services within the same room.

Access Control

Generic user names

Generic or shared user names should be limited in usage and scope. Exceptions may be limited to in the form of prospective learners within a controlled environment, static presentations services such as displays.

Temporary user accounts

Temporary user accounts may be used in limited circumstances such as supply teachers, whereby an audit trail is maintained. Access restrictions and clearance is still required before issuing along with the principle of least privilege.

Privileged accounts

Privileged or elevated accounts should be issued explicitly rather than for a norm due to the potential loss of confidential data and system resilience. Delegation should be utilised where additional privileges are required and interactive sessions should be limited.

Authorisation

Staff users who are granted access to IT systems are provided with email access, appropriate third-party access such as VLE, room booking system. In addition to storage in the form of H: drive and access to shared resources.

MIS access is also provided where necessary including access to restricted and sensitive data such as finance and HR.

Learners are provided with a user account, access to personal and shared network resources including access to an email account via a VLE. Additional VLE access third party may be issued depending upon the department in question.

Internet access

Staff internet access will be monitored in accordance with the agreed acceptable usage policy. All associated access will be recorded against a user name with regular monitoring.

Learners' internet access is filtered to safeguard users against any threats and harmful content whilst adhering to Prevent Duty Legislation. With Real-Time content filtering and regular reporting provides a mechanism to be responsive in addition to filtering access.

Additional monitoring software is employed within an IT suite help supervise and demonstrative purposes.

Remote Access

Remote access to School IT systems are available to both teaching and non-teaching staff via a web access gateway utilising Microsoft's Remote Desktop Services. Additional documentation and user training will be provided.

Whilst the remote access services are secured via a secure connection, all precautions should be made to access the service from a trusted host and network. The service operates as a gateway to IT Systems and provides no access to the host in terms of shared resources.

Application and software management

All software management must be undertaken by IT with additional software approved for use and documented. The illegal use of software is provided whilst appropriate licencing should govern the deployment of software.

Additional software control should be management within a group policy environment. This managed approach should limit the potential threats from document-based threats, help standardise systems and automate deployments.

Application network traffic should also be controlled by internet filters and firewalls to ensure all traffic is legitimate and meets the data protection standards.

Anti-virus software

Anti-virus software and endpoint protection is a critical tool against a variety of malicious threats, breaches of information and availability of IT systems. Whilst endpoint protection installation is automated, the failure to utilise such software raises the risk data and the IT systems hosting the services.

Patch Management

Patch management is an important tool against reducing the exposure against vulnerabilities in operating systems and applications. Therefore, patching as soon as appropriate testing can be completed should lead to fewer vulnerabilities there are to be exploited.

Emails

The use of emails must adhere to the acceptable usage and communications policies. Whilst no sensitive or confidential data can be sent without the use of encryption software such as egress secure email and file transfer.

Use of Encryption and Certification services

Encrypted storage should be deployed where sensitive and confidential data is stored. Encrypting the transportation such as remote desktop services should also be employed.

Both internal and external certification services should be utilised to identify devices, users and any services.

Any data transferred to third part services such as Capita should be transported via encrypted communications methods with data encrypted to the minimum of AES 256 standard.

Wireless connectivity

Domain services exposure to wireless networks should utilise appropriate safeguards such as WPA2-Enterprise with 802.1x authentication. The use of pre-shared keys should be limited to guest wireless access if additional authentication methods such as a captive portal is impractical.

Business continuity

Backup

A comprehensive backup schedule should utilise both hot and cold storage techniques such as mechanical hard drives and tape media. To ensure that data and software can be recovered following a media or systems failure, copies of all essential data must be taken at regular intervals.

Disaster recovery

Appropriate backups and replication of live data must provide an alternative provision in the requirement for the recovery and continuity of services. Failover testing and backup validation is required to ensure adequate resources are in place.

Virus outbreaks

Any sources of virus outbreak should be isolated from the network as soon as the infection is reported by the endpoint or staff member. If the threat is not cleanable by the endpoint software, the device should be isolated and cleaned appropriately.

Additional measure to ensure network segmentation via VLAN's should be employed to isolate various services such as guest wireless access.

Information security

All information should be considered and classified accordingly to an appropriate level of confidentiality, integrity and availability. Provision should be made on how and where the data is stored and transmitted. For example, appropriate sections on local network storage locations, MIS systems and distributed via the email system.

Leavers checklist

- All arrangement for access to data must be made before leaving
- Access control must be removed in addition to any fobs and assigned tokens
- Any equipment must be returned and provisioned
- User accounts disabled for local and externally hosted services
- Learners account should be disabled
- Data and emails archived in line with the retention policy