Our vision

Waverley School

Access Control Policy

November 2018

CONTENTS

Purpose

The objective of this policy is to minimise accidental or unauthorised access to School and/or partner connected systems, networks, applications, and information. It is applicable to all forms of logical access.

This document supports the School's Information Security Management System Policy and Code of Conduct for School workforce. It provides direction and support for the implementation of information security and is designed to help employees carry out the business of the School in a secure manner. By complying with this policy, the risks facing the School are minimised.

1. Introduction

Individuals who are not explicitly granted access to School information or information systems are prohibited from using such systems.

Individuals employed by or under contract to the School shall be granted access only to information and information systems that are required to fulfil their duties.

Access will be granted only to those staff who have formally agreed to comply with the School's Cyber and Information Security Policy and have signed the School's Acceptable Use Policy Code of Conduct (for School employees) or a confidentiality/non-disclosure agreement (agency workers).

This policy applies to:

- All schools workforce[1]
- Third party organisations who require access to the School information systems and facilities should also be aware of the contents of this policy.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the School Business Manager.÷

2. Physical Access Control

Control of entry into School buildings, sites and locations is important for the security of the School's information systems (both computerised and manual) and its employees. Control of entry into School buildings, sites and locations is important for the security of the School's information systems (both computerised and manual) its workforce and pupils.

Appropriate entry controls must be provided to ensure that only authorised persons are allowed access. This is best achieved through the use of an electronic ID card/pass system or the use of a signing in book where electronic control is not possible. Access control must be

[1] Applies to temporary and agency workers, volunteers, independent consultants and contractors – anyone working within the school environment in any capacity

rigidly enforced in buildings and areas housing sensitive information assets.

In buildings where IT facilities are located and where there is public access, special measures for access enforcement, particularly after normal office hours, must be taken.

3. IT Operations and Network Access Control

Access to information and information systems will be controlled on the basis of business and security requirements.

An access management process for every system/database must be created, documented, approved, enforced and communicated to all relevant employees and partner organisations.

Each business application run by, or on behalf of the School, will have a nominated system administrator who is responsible for managing and controlling access to the application and associated information.

Access to information must be based on "need to know" and segregation of duties and roles. The appropriate information, system, database, or application owner is the only individual that can authorise a systems administrator to grant or update access via the formal access management process.

Audit must monitor the process to ensure that access control is appropriately implemented according to ‘business need to know’ and ‘segregation of duty and role’ principles.

Special attention is given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

Access control requirements are clearly defined, documented and maintained by IT, who specify the rights of individuals or groups of users. Access control requirements are clearly defined, documented and maintained, and specify the rights of individuals or groups of users.

The School has adopted common windows-based operating systems, and predefined user profiles will be maintained to restrict access. The School has adopted common operating systems, and predefined user profiles will be maintained to restrict access. These access controls will be approved and reviewed by the data owner and occasionally reviewed by the Board of Governors to ensure consistency.

4. User Access Management

User access management covers all stages of user access, from initial registration, through changes in role, to deregistration and revocation of access.

The security of systems, networks, applications and databases is heavily dependent on the level of protection of user IDs, passwords, and other credentials that provide access to it. Hence, protecting the

credentials that provide access to information is indirectly protecting the information.

Identification and authentication of users and systems enables the tracking of activities to be traced to the person responsible.

All employees shall have a unique identifier (user ID) for their personal and sole use. Shared, group and generic user IDs are not permitted unless they are used to access the intranet only. Users must be educated that they are not permitted to allow their user ID to be used by anyone else. Users must be made aware of this and how to store them.

A process must exist for issuing and revoking the user IDs. Redundant user accounts must be monitored and managed.

5. User registration

A process for user registration and granting access rights exists and includes:

- Unique user IDs assigned so that access and modifications can be traced.
- Authorised users are aware of their responsibilities for the protection of information within the application and where applicable users sign an appropriate agreement.
- Ensuring access is granted once authorisation is obtained.
- Maintaining a record of all registered users.

Change of Role

Where an employee changes role within the School the following process is followed:

- Line managers must inform all relevant information owners/system administrators of the names of users that have transferred to different job/roles within 24 hours of transfer.
- Information owners must review the transferee's access rights to their systems to ensure that they are still valid.

6. Review of Access Rights

The data owner must approve access rights prior to set up by the system administrator.

IT does not have the authority to decide who should have access to what information. This is a business decision.

7. Removal of Access

On resignation of employment, line managers, in conjunction with HR, will undertake a risk assessment and determine whether existing access rights of an individual should be reviewed and reduced whilst working out their notice. Hostile terminations must be communicated to system administrators immediately and access immediately disabled.

Managers must inform IT of the names of employees that will be leaving School/partner employment at least 48 hours before the end of their last working day.

Access rights should be disabled by 5.00 pm on the employees lasting working day.

It is the responsibility of the School Business Manager to ensure that leavers return their entry ID pass at the end of their last working day and to return it to IT for deactivation as well as return all School ICT equipment that could be used to gain network access.

8. Password Management

Passwords are the key means of validating a user's authority to access a computer system. The following controls will be in place to ensure strong password management.

- Password length must be a minimum of 8 characters.
- Where the software solution allows the password, complexity will be as follows (or at minimum a combination containing at least three of the following conditions):
    1. One Numeric (0 1 2 3 4 5 6 7 8 9)

2. One upper case (A B C D E F G H I J K L M N O P Q R S T U V W X Y Z)
3. One lower case (a b c d e f g h I j k l m n o p q r s t u v w x y z)
4. One special character (* ! # . @ # $ % ^ & * ,)

- The password will be changed every 60 days (where the application allows this to be enforced, otherwise users will be required to change the password manually).
- Users should not repeat the same password within a cycle of 20 password changes.
- When an invalid password is entered three times in a row, the system revokes user access and must be reset. In some systems, users can do this for themselves using validation such as messages to mobile or secret questions. In others, system administrators must validate the request before resetting the password. Passwords stored on a computer are encrypted and protected from unauthorised access or deletion.
- Passwords must not be displayed on screen at any time.
- All default passwords must be changed following the installation of any new software or hardware.
- Users can reset their own passwords in some systems, in others, only system administrators are permitted to reset passwords or assign new passwords.
- New passwords and reset passwords are random and force immediate change after first login by the user. IT must ensure that they divulge new or reset passwords only to the authorised user of that ID.
- When it is known or suspected that a user ID has been compromised then IT must be immediately informed in order to have it revoked that and a security incident can be logged.
- System passwords, including administrator passwords that are used to access data that is required by the business, must be stored in secure locations such that in the advent of a business requirement the passwords can be recovered.
- There is a process in place to allow for the prompt resetting of passwords.

9. Privilege Management

A process is in place for the allocation and removal of system administration level access or increased user privilege and includes the following controls:

- Every level of privilege within each application and the categories of staff to which they need to be allocated are identified and recorded.
- Privileges are allocated to an individual as an event requires.
- Authorisation is recorded for each allocated level of privilege and only granted once authorisation is obtained.
- The development of system routines are identified and implemented to avoid the use of privileged access.
- Privileges are assigned to a different user ID from those used for normal business use and where possible a log of increased user privilege is recorded.

10. Monitoring System Access and Use

Systems will be monitored to detect deviation from the Access Control Policy and record events to provide evidence in case of security incidents.

IT establish the logging and monitoring requirements for business auditing purposes. and must establish the logging and monitoring requirements for the relevant purposes:

- Security
- Incident investigations
- Audit
- Fraud
- Legal

A process for capturing logging and monitoring requirements must be developed. Audit and event logs will need to be adequately secured, possibly centrally and separately from privileged-level employees (separation of duties). Tools may be required for log analysis.

11. Security of Third Party access

School employees responsible for negotiation, initiation, authorisation, implementation and maintenance of third party relationships and services pertaining to the School must consider factors relating to:

- Legal and regulatory requirements
- Contractual obligations
- Security policy requirements
- Information governance requirements
- Network operations must be identified, understood and approved via a risk assessment.

12. Access from overseas

Access to School's network from overseas is subject to additional controls to ensure compliance with relevant legislation, including the Data Protection Act, and this will place additional personal liability on users.

ICT equipment supplied by the school may only be taken to EEA countries and those identified as having an assessment of adequate data protection by the ICO or School. See the ICO page:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

Note that the above applies equally to School owned devices and personal devices with ability to access council data (i.e. BYOD).

13. Access to Secure Areas

All network equipment (including, but not limited to WAN service termination equipment, routers, switches, cabling patch panels) will be kept in appropriate locked facilities whenever practicable. All network equipment outside of designated communication rooms must be kept securely. Staff must ensure that communications cabinet and communications room doors are secured when they are left unattended. All keys must be limited to staff who need them to carry out their duties. If any key is lost or mislaid, or any door found unlocked, then this must be reported immediately as an IT security incident.

All physical servers must be kept physically secure in an area for authorised individuals only. A process of allocating and monitoring access to server rooms must be implemented – this may include electronic access control or the use of signing in books as appropriate.

For cloud servers and services, the supplier must have a suitable Cloud Security Assessment (see Use of Cloud Services Security Policy).

14. Policy Compliance

The School requires that all employees comply with the directives presented within this policy.

Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to any person.

- If complying with the policy would cause significant damage to the school's reputation or ability to operate.
- If an emergency arises.

In such cases, the user concerned must take the following action:

- Ensure that their manager is aware of the situation and the action to be taken.
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report.
- Ensure that the situation is reported to the office and the Headteacher as soon as possible.
    - Failure to take these steps may result in disciplinary action.

In addition, IT will maintain a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified.
- Minor breaches that are not considered to be worth rectifying.
- Any situations to which the policy is not considered applicable.

The School will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

15. Penalties

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy.
- Unauthorised disclosure or viewing of confidential data or information belonging to the School or partner organisation.
- Unauthorised changes to information, software or operating systems.
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body.
- The exposure of the School or partner organisation to actual or potential monetary loss through any compromise of security. The exposure of the school or partner organisation to actual or potential monetary loss through any compromise of security.

- Any person who knows of or suspects a breach of this policy must report the facts immediately to the Headteacher.

Any violation or non-compliance with this policy may be treated as serious misconduct.

Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.