Ormiston Sandwell Community Academy

Ormiston Academies Trust

Network Access Policy

Policy Version Control

Policy type	Internal OAT Policy
Policy prepared by (name and department)	James Miller, ICT
Last review date	October 2015
Description of changes	New policy
Name and date of line manager's approval	James Miller - 22/10/2014
Date of executive approval	22/10/2014
Date released	22/10/2014
Next review date	22/10/2015

Contents

1. Policy statement and principles

1.1 Policy aims and principles

This policy is to ensure that the information held either onsite at OAT head office / stored in remote locations / academies is secure and the privacy is maintained at all time. It explains the importance of appropriate access and security of electronic data.

This policy is consistent with all other policies adopted by the academy and is written in line with current legislation and guidance.

1.2 User Account Definitions

The following defines the types of computer user logon accounts:

End user

The majority of *staff / students / parents* will be an 'end user' with an IT system account that will allow access to private email, internet, personal storage and team storage of files and folders.

Enhanced user

This user will have all the properties of an 'end user' but will also be granted 'local Admin' for their IT device, allowing users to change device settings at a hardware and operating system level.

Network Administrator

This account will be used by OSCA's IT support staff who are responsible for the maintenance of computer hardware and software systems that make up the computer network including the maintenance and monitoring of active data network, LAN/WAN infrastructure and related network equipment. This account will not allow access to end user email or personal storage areas.

Domain Administrator

This account is used to manage the replication of directory information within the Active Directory, and makes any enterprise level changes to the Active Directory, such as Active Directory modifications. It is a privileged access account granting access to all of the network information and user files, folders and emails, therefore it can only be used when following the protocol set out in 3.4

1.3 Data Storage Areas

OSCA has 3 server rooms located at 3 different locations on the school site.

1.4 Complaints

All complaints are dealt with under the **OAT Complaints Policy**.

Complaints should be made in writing and will follow the OAT complaint procedures and set timescales. The handling of complaints may be delegated to an appropriate person.

The outcome of the complaint will be communicated in writing.

1.5 Monitoring and review

This policy will be reviewed annually or in the following circumstances:

- Changes in legislation and / or government guidance
- As a result of any other significant change or event
- In the event that the policy is determined not to be effective

If there are urgent concerns these should be raised to OSCA's E-safety Working Group in the first instance for them to determine whether a review of the policy is required in advance of the review date.

2. Roles and responsibilities

2.1 Key personnel

Mr D. Dumbell		Vice Principal (Data and Standards)
Contact Details	Email	David.dumbell@ormistonsandwell.org.uk
	Telephone	0121 - 5525501
Mr D. Fones		Network Manager
Contact Details	Email	Darren.fones@ormistonsandwell.org.uk
	Telephone	0121 - 5525501

3. Network access and use

3.1 Appropriate use of Network Administrator

Access to computing resources should only be used for official academy business. Use of Network Administrator Access should be consistent with an individual's role or job responsibilities.

3.2 Inappropriate use of Network Administrator

In addition to those activities deemed inappropriate in the [OSCA's Employee Code of Conduct/ Student Code of Conduct], the following constitute examples of inappropriate use of Network Administrator access to the academy computing resources unless otherwise documented and approved by OSCA's Governing Body:-

- Knowingly changing or acquiring user access to any other users network account
- Knowingly accessing protected or prohibited data online or on the academy network
- Accessing protected or prohibited data that is outside the scope of specific job responsibilities
- Knowingly allowing access to, exposing or otherwise disclosing protected or prohibited data to unauthorised persons
- Using access to gain restricted information about an individual, system, practice, or other type of entity

3.3 Passwords

It is the user's responsibility to keep their passwords safe. Staff members are not to share password information with anyone unless directed to by the principal. No user passwords are to be stored or shared by any individual. If for any reason forced access is required to a user's account the network administrator with the express permission of the principal will change the password of the user to an agreed password. This action will be documented.

Note: The documentation of such an event will not include any password information only that of whose account has been changed and the person who made the request.

3.4 Domain Administrator account access protocol

The account will not be used by ICT staff unless deemed an emergency or necessary for completing a specific planned task as set out below.

Planned usage

Planned usage is defined as an event prepared for before it happens. This access must be agreed with the Vice Principal (Data and Standards) and the IT network team.

In the event of this being used the staff member must document the date, time, reason for access and feed back to the principal.

Emergency usage

Emergency is defined as a situation that can only be resolved by domain level access, such as dealing with a virus, recovering from a serious hardware / software failure. In the event of an emergency ICT staff will request use from the Vice Principal (Data and Standards) and the IT network team and then access the account. In exceptional circumstances e.g. contact cannot be made with the Vice Principal (Data and Standards) and the IT

network team the domain password may be manually reset.

In the event of this being used the staff member must document the date, time, reason for access and feed back to the principal.

Reset of password for domain account

The domain password will be retained by the IT support team only.

Upon use by the ICT team, the password will be reset at the earliest opportunity by the IT support team only.

Note: It is expected that all possible alternatives will be considered and where appropriate attempted to resolve the issue prior to this access being used.

3.5 ICT Support Team

Each ICT support team member will be provided with two accounts.

- Standard User account
  - This will be the 'end user' access account and must be used for all non-administration access
- Network Administrator account
  - This account will be provided with appropriate rights to ensure that the member of staff can perform all of their expected administration tasks
  - This account should only be used when logging onto servers or when elevating access.
  - This account is not to be used as an everyday user

3.6 Third party support SMIS have a local admin account to use when they address school MIS problems.

Any external company who supplies support will be provided with an account appropriate for the support needs. This account will be activated when required and disabled at all other times. This access must be agreed giving clear times of access and clearly stating the areas to be accessed. Any external access to any academy service or resource will be logged by the ICT Team and reviewed by the e-Safety Working Group.

3.7 Email mailbox access

User email accounts will be given exclusive user access permission only, unless delegation is documented and approved by the Principal.

Shared email accounts will be formally requested, documented and approved by the principal before being created and delegated exclusively to the appropriate users.

3.8 Transparency of Network and Domain Administrator Account usage

The academy IT computer network has an audit logging feature which will be used to record file, folder and email access by all users. When a user opens a file or folder a record is added to event log. The event logs will in time become very large, therefore event logs can only be kept for 90 days. The principal can request reports

from the audit log.

3.9 Backup file access

Encryption of the backed-up data enables safe transport and storage. All backup data must be encrypted and treated the same as 1.3

The passwords or keys are required to be kept separate from the data itself.

3.10 Reporting inappropriate use of academy computer accounts

Any user who suspects a violation of computer security should contact the principal. This includes suspected inappropriate use of IT accounts.