**Provisioning Privileged IT Accounts**

[Insert School Name]

[Version]

|  |  |
| --- | --- |
| **Last Reviewed** |  |
| **Reviewed By** |  |
| **Next Review Date** |  |

**Contents**

[Purpose of this document 2](#_Toc63433422)

[Types of Administrative Accounts 3](#_Toc63433423)

[Data Integrity 4](#_Toc63433424)

[Monitoring 4](#_Toc63433425)

[Appropriate Use of Administrator Access 4](#_Toc63433426)

[Reporting Requirements 4](#_Toc63433427)

[Exceptions 4](#_Toc63433428)

[Annex 1. Provisioning Process for Privileged Accounts 6](#_Toc63433429)

[Annex 2. Example Administrator Account Log 7](#_Toc63433430)

# **Purpose of this document**

Network and systems administrators have privileges and duties that may bring them into contact with sensitive, restricted or personal information during the course of their work.

The purpose of this document is to ensure that administration roles and responsibilities are properly understood and that privileged accounts are used appropriately.

These guidelines apply to all personnel, including those providing services under contract, who are provided with **Administrator or Privileged Access** to school computing and information resources. This includes school systems and individual software applications.

**Privileged User Definition**

Anyone with access that enables them to affect change which would be felt beyond their immediate job role could be considered a privileged user.

*For example:*

Administering systems or networks which are critical to a business (e.g. database admins)

**OR**

Accessing systems used to perform a critical function (e.g. approving financial payments)

Taken from the National Cyber Security Centre (NCSC)

**Privileged Access is therefore defined as a level of access above that of a normal user.**

Examples of users with privileged access:

* A School Business Manager account with the ability to process payments.
* An external IT Support Technician account providing access to the server.
* A DSL account with read/write access to a safeguarding reporting application.
* A curriculum subject leader account with access to add/remove users from a curriculum app.

Privileged user accounts have specific additional access on one or more systems or applications and should ensure:

1. These accounts should have unique and complex passwords (at least 8 characters with an automatic deny list or MFA enabled, or a password of at least 12 characters).
2. It is necessary to continuously monitor admin account use and periodically review access.
3. Schools should keep a documented record of staff granted enhanced access to systems and which system the access relates to.
4. Privileged accounts should be in addition to a user’s standard account and NEVER used for routine functions.

# **Types of Administrative Accounts**

1. **Local Administrative Accounts** are non-personal accounts that provide administrative access to the local host or instance only.

*Example: Staff member who has been given an admin account to make changes, add users, or perform maintenance on a specific workstation or laptop.*

1. **Application Administrative Accounts** are accounts used by applications to access databases, external third party applications or services.

These privileged accounts usually have broad access to underlying company information that resides in applications and databases.

*Example: Administration staff with write access to the schools Management Information System (MIS)*

1. **Domain Administrative Accounts** have privileged administrative access across all workstations and servers across the domain (school IT network).

These accounts provide the most extensive access and any compromise to the security of this type of account is serious and puts the school at risk*.*

*Example: An IT Technician who monitors connectivity and implements group policy across the whole network.*

1. **Emergency Accounts** provide unprivileged users with administrative access to secure systems in the case of an emergency and are sometimes referred to as ‘break glass’ accounts.

The schools Incident Management and Disaster Recovery Plan should detail when and how an emergency account should be provided. Access should be documented for auditability.

It is recommended that there is one additional user with privileged access for each system, which reduces the need to make sudden decisions in an emergency.

*Example: Staff illness prevents admin access and the school can’t provision new accounts or make system modifications. A new admin account is needed to maintain the functionality and core business functions.*

User accounts should always follow the ‘least privilege’ principle. Only provide users with accounts which provide sufficient access for the requirements of their role.

**Staff should have separate user accounts if they are expected to perform both administrative and routine functions.**

Administrators should log in with their standard user accounts for day-to-day tasks.

**Data Integrity**

Administrators must ensure their activities do not result in the loss or destruction of information.

If a change is made to stored data then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

# **Monitoring**

Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users that both such monitoring will be carried out, and the policies to which it will apply.

If this has not been done through a general notice to all users (such as a staff acceptable use policy and agreement) then individual permission must be obtained from file owner(s) before a file is examined. If a network communication is monitored all parties should provide consent before any monitoring takes place.

# **Appropriate Use of Administrator Access**

The privileges provided to administrators are solely for the purposes of supporting the smooth running of the school and to enable the school to ensure maximum availability, data integrity and security for the systems they are responsible for.

The use of Administrator Access should be consistent with an individual’s role or job responsibilities as prescribed and authorised by school senior leaders. When an individual’s role or job responsibilities change, Administrator Access must be reviewed and appropriately updated or removed.

In situations where it is unclear whether a particular action is appropriate, and within the scope of current job responsibilities, the situation should be discussed with the Headteacher.

# **Reporting Requirements**

Report any suspected violation of the School IT Security Policy to the Headteacher. This includes suspected inappropriate use of Administrator Access.

Report any data or security breach concerns to the Headteacher promptly, providing information as to the date, time, location and potential extent of any breach.

Significant data breaches may also need to be reported to the Information Commissioner’s Office (ICO) within 72 hours.

# **Exceptions**

Requests for exceptions to any information security policies may be granted for documented and explicit reasons with compensating controls in place to mitigate risk.

**Administrator Acceptable Use Agreement**

System administrators **must**:

1. Restrict the use of accounts with privileged access to only school functions consistent with the administrator’s role, job responsibilities, and the purpose for which the access was granted.
2. Ensure that networks, systems and services are available to authorised users only.
3. Ensure information is handled and transferred correctly, preserving its integrity and providing an appropriate level of security for the classification of the data being processed.
4. Ensure that default passwords are changed using strong password methodologies when an Information System is installed or implemented.
5. Where necessary, monitor compliance with IT policies which apply to the systems being administrated and act in support of school policies at all times.
6. Monitor and record network traffic if defined as being in the scope of the role.
7. Take steps to ensure adherence to, and compliance with, all hardware and software license agreements entered into and communicated by the school.
8. Examine relevant files as part of necessary security investigation if defined as being in the scope of the role.

In addition to those activities deemed inappropriate in the school’s Acceptable Use Policy, Administrator’s **must not**:

1. Bypass user access controls or any other formal security controls, without documented approval.
2. Bypass formal account activation, suspension or change procedures, including enhancing user permissions without authorisation.
3. Bypass security measures or access restrictions applied to protect information, or accessing information that is outside the scope of specific job responsibilities.
4. Disclose information, accessed as part of authorised works, to those unauthorised to view it.
5. Use additional access to satisfy personal curiosity about an individual, system or school practice.
6. Monitor user activity which is not authorised and/or does not form part of routine monitoring encompassed by school policy.
7. Use administrative accounts when there is not a business need to do so.
8. Make changes or modifications to systems or services without prior SLT approval.
9. Attempt to make readable the content of a file or communication which appears to have been deliberately protected by the owner, for example by encrypting it, without specific authorisation from management or the owner of the file.
10. Use privileged accounts for reading email or browsing the web.
11. Use administrative credentials to access systems with untrusted devices.

I have read the guidelines for Privileged IT Accounts and agree to abide by the Acceptable Use of Administrative Accounts.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Job Role:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorised by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Job Role:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authoriser Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Annex 1. Provisioning Process for Privileged Accounts**

1. Governors confirm a new appointment to a post or the change of a role which requires additional access.
2. [School Business Officer] completes a new starter form, if relevant, and signposts / provides the user with copies of relevant policies and acceptable use agreements.
3. [School Business Officer] ensures both the standard user **and** administrative user agreements have been signed and appropriately archived.
4. [School Business Officer] formally requests additional access for the user by emailing the request to the [Headteacher].

The request should include:

* The name of the user
* The role of the user
* A list of all systems enhanced access is requested for
* A brief reason for the addition access
* A scheduled review term or a fixed review date for temporary/emergency access.

1. The [Headteacher] confirms approval of the access via email, confirms the **level of access** and requests provisioning from [IT Technician / Business Officer].
2. [School Business Officer] adds the user to the Administrator Account Log with details of the system and the review period.

The following should trigger an automatic review of access and consideration for revocation:

* Notice to leave a post
* A change of role
* Contractual expiry
* Breach of policy or user actions which may lead to disciplinary action

Further support is available from the NCSC – [Managing User Privileges](https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges)

# **Annex 2. Example^ Administrator Account Log**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Role** | **System** | **Authoriser** | **Authorisation Date** | **Review** | **Access Revocation** | **Revoked By** |
| John Smith | Business Officer | RM Integris | B. Nadin (Headteacher) | 7th Sept 1999 | Annual + COC | 30th March 2007 | K. Lyme  (Headteacher) |
| Jane Allis | DSL | MyConcern | K. Lyme (Headteacher) | 16th Feb 2015 | Annual + COC |  |  |
| Dale Yarrow | IT Technician  (External Company) | Server Maintenance | P. Clarke  (Chair of Governors) | 3rd Sept 2017 | 6 Monthly + Contractual Change | 1st August 2018 | Kate Johnson  (Business Officer) |
| Kate Johnson | Business Officer | RM Integris | K. Lyme (Headteacher) | 22nd June 2019 | Annual + COC |  |  |
| Pete Derry | IT Restoration\* | File Server | P. Clarke  (Chair of Governors) | 4th Aug 2020 | 20/09/2020 | 21/09/2020 | Kate Johnson  (Business Officer) |
| Lee Graham | IT Lead | TT Rockstars | K.Lyme (Headteacher) | 8th September 2020 | Annual COC |  |  |

\*COC = Change of Circumstance

\*Detail if access is job specific and set fixed review dates

^ Names are fictional