Email and Computer Network Access (Staff) Policy

Written by:	Marcus Link	**Date:**	February 2018
Approved by:	College of Management	**Date**:	
	Council of Trustees	**Date**:	

Review information: Version 1 developed by ML and GW.

Date for review: September 2018

Statement of Intent

The aim of this policy is to ensure, so far as is reasonably practicable, that the school can provide email and file sharing facilities for its staff and keep these in line with current data protection legislation.

Policy

Policy Statement

- The school operates a variety of IT services to enable staff to access contact information, pupil related data, use email, share files, scan, copy and print documents.
- These services are provided locally on the school site and some via remote access.
- The school constantly strives to improve its IT infrastructure which at this time remains fragmented and basic.
- This policy focuses on access to email services and file sharing environments.
- Every member of staff will receive at least basic user access to one personalised email account and a user account for the school's main computer network
- All users will ensure that confidential information is kept only in the relevant areas of the system and will report any breaches promptly
- All users will not share their access information including any passwords to any other person unless requested to do so by one of the superuser along with confirmation of this request by a (separate) member of the SLT
- All members of staff can access their emails and files via the network locally and via remote access

School Email Addresses

- The school uses Google Apps for the majority of its email accounts along with services provided by the Microsoft 365 service.
- These addresses are managed by the school's superusers.
- Members of staff and trustees are required to use their school email addresses for all school related email communication.
- If members of staff and trustees receive school-related emails to email addresses other than their school email address, they should forward this to their school email address and respond from there.
- In any case, members of staff and trustees should refrain from prolonged use of email addresses other than their school email addresses.

Roles and Responsibilities

Named IT Contractor

- The school's networks are managed remotely by the school's chosen IT contractor AME Solutions, Exeter.
- AME can be contacted by email support@amesolutions.co.uk or telephone 01392 824022.
- AME will use the key members of staff pages on the school's website for verification along with the current network user profiles and access levels when considering any request.
- AME does not generally support the school's email accounts. These are managed internally by the superusers.

Trustees/ Directors

- Members of the Council of Trustees are the trustees of the charity and directors of the company and there are public records on the websites of the Charity Commission and of Companies House.
- As the trustees/ directors generally do not work at the school and do not have user accounts at the school, they do not generally have access to the school's network.
- However, as the trustees/directors, they have in principle access to all areas of the system excluding Safeguarding which is accessible in principle only to the trustee with safeguarding responsibility.
- Trustees/ directors may request access to the school's network at any time.
- In order to grant such a request, a second trustee/ director is required to confirm the request.
- AME will use the key members of staff pages on the school's website along with public records listed above to verify the legitimacy of any such request.

User Levels

The school has four different layers of users: basic users, advanced users, guest users and superusers.

- **Superusers**
    - Superusers are responsible for the maintenance, upkeep and caretaking of any email and network systems used by the school whether these are located on-site, offsite or on the web
    - Superusers liaise with school's IT contractor AME
    - Superusers create, edit and remove any email and network user accounts
    - Superusers can create, edit and remove basic user accounts
    - When requesting the creation or change to any advanced user, guest user or superuser, two superusers or one superuser and the DSL or one other member of the SLT or member of the Council of Trustees are required: one to request (usually but not always the superuser) and the other to confirm the request.
    - Superusers cannot request changes to their own user profile and access level.
- **Basic Users**
    - Every member of staff will receive at least basic user access to one personalised email account and a user account for the school's main computer network
    - Basic users have local and remote access to the network drives called ADMINISTRATION, EDUCATION and UNRESTRICTED
    - Basic users will ensure that no confidential information is kept on the above drives unless this has been deemed acceptable as per the below exceptions
    - The following documents are acceptable exceptions:
        - Risk assessments
        - Special needs and consents resumes for school trips and general use
        - ICE contact lists for general use and school trips
    - Basic users can access the network locally and remotely
    - Basic users are part pf the security group ST-Staff
- **Advanced Users**
    - Advanced users have access to one or more security groups outside of the guest and staff groups depending on requirements.
    - Advanced User status is required for access to the following drives:
        - Safeguarding (O:)
        - SMT (P:)

        - Finance (T:)
        - HR (V:)
        - Confidential (W:)
        - Imagefiles (X:)
        - Learning Support (Z:)
- **Guest User**
    - The guest user account has the username rudolf.steiner
    - The password is available to guest users is provided to any volunteer, member of staff, contractor, supplier or other user who may legitimately require access to a school computer.
    - This user is a member of the security group ST-Guest
    - It has access to the drive UNRESTRICTED

Access Levels

File Sharing

- Files are generally managed via the school's network local to Hood Manor which is managed AME on behalf of the school.
- The school operates the following top-level network drives for file sharing:
    - Safeguarding (O:)
    - SMT (P:)
    - Education (Q:)
    - Upper School (R:)
    - Administration (S:)
    - Finance (T:)
    - HR (V:)
    - Confidential (W:)
    - Imagefiles (X:)
    - Unrestricted (Y:)
    - Learning Support (Z:)
- These are accessible locally via the school's network in Hood Manor and remotely via the Internet with an appropriate user account.

- The Upper School, Visiting Students and Summer Language School departments use Google Drive and its successor services to manage file sharing as key members of these functions do not generally have access to the local network in Hood Barn.

Security Groups

- These are managed AME on behalf of the school.
- The school has the following security groups:
    - **ST-Guest**
      This includes the guest user which is not included in any other group and has access only to the drive "unrestricted".
    - **ST-Staff**
      Default group for any basic user
    - **ST-Finance**
      Finance team + ST-Executive
    - **ST-SMT** (to become ST-SLT)
      ST-Executive + Management Assistant
    - **ST-HR**
      ST-Executive + Payroll
    - **ST-Safeguarding**
      Safeguarding team
    - **ST-Executive**
      SMT without Management Assistant
    - **ST-Confidential**
      ST-Executive + DSL

Network Access Rights

- These are managed AME on behalf of the school.
- The network can be accessed by the security groups in the following way:
    - **Safeguarding**
      Accessible to members of the safeguarding team only.
    - **SMT** (to be renamed to SLT)
      Accessible to members of executive and the Management Assistant only.
    - **Upper School**
      Accessible to all staff.

- **Administration**
  Accessible to all staff.
- **Finance**
  Accessible to finance staff and executive team.
- **HR**
  Accessible to payroll, personnel staff and executive team.
- **Confidential**
  Accessible to executive team and DSL.
- **ImageFiles**
  Accessible to all staff.
- **Unrestricted**
  Accessible to all staff and ST-Guest.
- **Learning Support**
  Accessible to executive team and ed support team.

Controls

- Health & Safety Induction and Annual Confirmation
- Key members of staff pages on the school's website (www.southdevonsteinerschool.org)

Information/advice/guidance:

-

Compliance:

- Computer Misuse Act 1990
- Data Protection Act 1998

Linked Policies:

- Data Protection Policy