

Denefield School Email System Policy

1.0 Purpose

The purpose of this email policy is to ensure that all Denefield employees are aware of the Governors and SLT expectations of them when using the school's email system.

This is to prevent tarnishing the public image of Denefield School when email is sent externally from the school email system as well as setting out the frame work for acceptable use.

2.0 Scope

This policy covers the use of the school email system, either on the premises or accessed remotely.

3.0 Policy

3.1 Prohibited Use. The school email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including, but not limited to, offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content should report the matter to their supervisor immediately.

3.2 Personal Use.

It is acceptable to use the school email system for personal email but policy sections 3.1, 3.3, 3.4 and 3.5 are still applicable.

3.3 School image

Employees should keep in mind at all times that email sent from a school account can and will be viewed as school policy and any statements, promises or information contained therein must be checked and agreed before transmission.

3.4 Monitoring and data retrieval

Denefield employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Access to email accounts for monitoring purposes or for the purpose of retrieving information while an employee is absent or has left the school requires written permission from the head and will only be carried out if there is reasonable evidence the employee has breached the prohibited use policy or written permission from the employee has been received. Any such access to e-mail must take into account the Employment practices code as set out in the Data Protection Act and must not contravene The Regulation of Investigatory Powers Act or the Lawful Business Practice Regulations.

3.5 Transmission of sensitive data

At no time should information about a pupil be emailed externally to anyone other than that pupil, the pupil's parent or guardian or the Local Authority and must take into account the relevant sections of the Data Protection Act.

When communicating with parents by email, other pupil's names, unless they are siblings, should not be used. The use of other teachers' names should be avoided but if this is not possible permission from that teacher to use their name must be sought. When transmitting sensitive data appropriate safeguards should be put in place such as password protected files.

4.0 Security

It is every employee's responsibility to ensure that no other employee or third party can access their e-mail account either in school or from an external pc or handheld device. The sharing of passwords is prohibited.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.