High Grange

Adaptive thinking, Communication, Emotional wellbeing, Independence

Creating a Safe Environment		
Electronic Communications Policy		
Last Update: **September 2025**	Responsible: **Principal**	Page: **1 of 4**

This policy promotes ACE because;	
	This policy supports ACE by promoting adaptive digital thinking, modelling respectful communication, safeguarding emotional wellbeing through clear boundaries, and enabling independence within secure systems. Staff demonstrate responsible digital citizenship, helping students learn how to use technology thoughtfully, communicate professionally, stay safe online, and develop confident, responsible habits as their independence grows.

Contents

1. Purpose and Scope

This policy outlines expectations for the appropriate and lawful use of all electronic communication systems at High Grange School, including:

- School computers, tablets, and phones
- Email and voicemail
- Internet access and online platforms
- Messaging systems
- Social media and blogging

The examples provided within this policy are not exhaustive and aim to provide a wide scope to cover Highgrange School's operations in the education sector.

It applies to all employees, volunteers, and contractors using school-provided or personal devices on school premises or networks.

2. Core Principles

- All digital systems are the property of the school and must be used only for authorised, professional purposes
- Inappropriate, illegal, or personal use is prohibited
- Electronic communications must uphold safeguarding, confidentiality, and professional conduct standards
- All use is subject to monitoring and must comply with legal duties under UK GDPR, The Human Rights Act, and The Telecommunications (Lawful Business Practice) Regulations 2000

3. Acceptable Use Guidelines

Permitted Use:

- Teaching, planning, and school administration
- Communication with staff, parents, or external professionals for school purposes
- Access to safeguarding platforms and digital learning tools

Prohibited Use:

- Personal browsing, gaming, or non-work email during work hours
- Accessing, creating, or forwarding offensive, indecent, discriminatory, or defamatory content
- Use of school accounts or devices for private business or unauthorised social media activity
- Downloading unapproved software, music, games, or copyrighted material
- Using communication tools to harass or intimidate others
- Staff must not install unapproved software or copy school-owned programs. All files must be virus-checked by authorised personnel before being added to the school network. Passwords must be kept secure and not shared under any circumstance. Should access be required for accounts then a password reset request will be raised with the appropriate member of staff.

4. Email and Messaging

Staff must:

- Use only school-issued email accounts for work-related communication
- Maintain a professional tone in all emails and digital messages
- Not transmit sensitive or confidential data without encryption or authorisation
- Avoid replying in haste, using informal or inappropriate language, or sending messages that could be interpreted as bullying or discriminatory
- Include a disclaimer in external messages where required

All email content is considered school property and may be accessed, archived, or audited in line with policies & procedures.

Email should not replace face-to-face communication where appropriate. Staff should avoid “flame-mails,” hasty responses, or irrelevant group-wide emails that may lead to misunderstandings or disrupt professional working relationships.

5. Internet Access

- Internet use must be related to professional duties or training
- Access to inappropriate websites (e.g. pornography, extremist content, violence) is strictly forbidden
- Social media platforms may only be accessed with prior authorisation for:
    - Curriculum delivery
    - Safeguarding responsibilities
    - School communications

Any accidental exposure to harmful or restricted content must be reported immediately to IT and the DSL. Including individuals involved, the date & time of the incident, nature of the content and platform the media was accessed from.

6. Social Media and Blogging

- Staff may not post content that references the school without prior approval
- If a personal social media account identifies the user as a school employee, a disclaimer must be included:
  "The views expressed are my own and do not reflect those of High Grange School."
- Staff must not share:
    - Confidential pupil or school information
    - Comments that are offensive, defamatory, or unprofessional
    - Content that could bring the school into disrepute

Any staff member found to be in breach may be subject to disciplinary action, up to and including dismissal.

Staff who blog or engage in personal social media activity that identifies them as affiliated with the school must inform their line manager and ensure content is aligned with school values. Paid blogging or promotional content should be declared. If in doubt about potential conflicts of interest or reputational risk, staff must seek guidance.

7. Telephone Use

Landline:

- School telephones are for professional use only.
- Limited personal calls are permitted only in emergencies or in exceptional circumstances.
- Lengthy or premium-rate calls are prohibited.

Mobile Devices:

- School-issued mobiles must be used only for school business.
- Personal use is permitted only in emergencies or in exceptional circumstances.
- Staff may use their mobile phones offsite should they need to contact the school or as above in an emergency.
- Lost or damaged phones due to negligence may result in cost recovery from the employee.
- In line with legal road safety guidance, staff must not use mobile phones while driving unless the vehicle is parked in a safe location. Hands-free use is not considered safe during motion.

8. Monitoring and Oversight

The school reserves the right to monitor email, internet usage, phone calls, and network activity. Monitoring is carried out in line with legal frameworks and aims to:

- Ensure effective operational use
- Detect misuse & unauthorised access
- Protect system security
- Safeguard children and staff
- Inform best practice and positively influence quality control
- Support disciplinary investigations

Monitoring may include access to staff emails, phone logs, and internet browsing history. All monitoring is proportionate, confidential, and in accordance with the law. Staff will be notified if additional consent is required. Records, logs and other recorded data will be processed, retained and disposed of in accordance with current Data Protection Legislation.

9. Confidentiality and Legal Risks

- Electronic communications are subject to the same confidentiality and legal standards as any other form of correspondence.
- Messages may be disclosable in legal proceedings.
- Staff are personally responsible for content sent via email or social media.
- Misuse of electronic communications may result in legal consequences including personal liability for defamation, privacy breaches, or unauthorised disclosure. Messages should always be composed with professionalism and care.

10. Policy Breaches

Failure to comply with this policy will be managed under the school's Disciplinary Procedure. Serious breaches (e.g. deliberate transmission of harmful material or disclosure of confidential data) may constitute gross misconduct and result in summary dismissal.

11. Review and Governance

This policy will be reviewed annually or earlier if prompted by legislation, safeguarding updates, or school-wide IT changes.