High Grange

***A**daptive thinking, **C**ommunication, **E**motional wellbeing, **I**ndependence*

Creating a Safe Environment		
Computer and Internet Access Policy		
Last Update: **September 2025**	Responsible: **Principal**	Page: **1 of 5**

This policy promotes ACE because;	
Adaptive Thinking Communication Skills Independence Emotional Wellbeing	This policy promotes ACE by modelling adaptive, responsible digital decision-making; establishing clear, respectful communication norms; protecting emotional wellbeing through safe, monitored systems; and enabling independence within secure boundaries. Staff exemplify professional online conduct, students learn safe digital citizenship, feel confident and protected, and develop habits that transfer across contexts effectively.

CONTENTS

1. Purpose and Scope
2. Access and Security
3. Acceptable Use Expectations
4. Email and Digital Communication
5. Online Safety and Safeguarding
6. Monitoring and Filtering
8. Use of Images, Videos and Copyrighted Content
8. Misuse and Disciplinary Action
9. Use of Personal Devices (BYOD)
10. Roles and Responsibilities
11. Breaches of Policy
12. Review and Evaluation

1. Purpose and Scope

This policy sets out the principles and rules for the appropriate use of High Grange School's IT systems, including computers, internet, email, and social media. It applies to all employees, volunteers, contractors, and visitors using school devices or networks.

It aims to:

- Promote safe, responsible, and lawful use of digital technologies
- Safeguard pupils, staff, and the school community
- Protect the school's IT systems and data

It applies to all users whether accessing school systems on-site or remotely. Staff are also expected to comply with the school's Electronic Communications Policy.

2. Access and Security

- School systems are only for authorised users
- Individual logins and passwords must be kept confidential and changed regularly
- Users must log off or lock their devices when unattended
- Shared files must be saved in appropriate network areas
- Downloading files or software must be authorised by the Network Manager to prevent the risk of malware or system compromise
- Users should never install or run unauthorised programs, as this may compromise system security or violate software licensing agreements

3. Acceptable Use Expectations

Users must not:

- Access, share or download illegal, offensive, or sexually explicit material
- Post or share abusive, discriminatory or threatening messages
- Use personal social media during working hours
- Share login credentials with others
- Install unapproved software or games
- Use school devices for personal profit, unauthorised social media, or political lobbying

School devices are monitored. Breaches of acceptable use may result in sanctions, disciplinary action or legal involvement.

Accessing personal social media accounts for non-school purposes is prohibited during working hours.

4. Email and Digital Communication

All school email and communication tools must be used professionally and lawfully.

Users must not:

- Send or forward inappropriate jokes, images or links
- Share sensitive or personal data without encryption or permission
- Use informal, abusive, or misleading language
- Use school email addresses for personal or commercial activity

Emails may be accessed, archived or monitored by the school for safeguarding and operational purposes.

Monitoring may include accessing staff email accounts when necessary to maintain continuity of communication during absence.

Messages sent via school systems may be retrieved even after deletion and can be used in disciplinary or legal proceedings.

5. Online Safety and Safeguarding

- Online safety is the responsibility of all staff
- Concerns about inappropriate content, cyberbullying, grooming or exploitation must be reported immediately to the Designated Safeguarding Lead
- Users must not attempt to bypass internet filters
- Staff must model appropriate online behaviour and language at all times

This policy supports duties outlined in Keeping Children Safe in Education (KCSIE), the Prevent Duty, and the Equality Act 2010.

6. Monitoring and Filtering

- The school monitors internet activity, device usage, and network access
- Monitoring systems are used to safeguard students, detect misuse, and support investigations
- The filtering system blocks harmful or unauthorised content
- Devices may be remotely accessed or locked by authorised personnel in line with safeguarding or legal duties
- All monitoring is lawful, proportionate and logged
- Monitoring may also include review of emails or files to ensure smooth operation during staff absence or technical issues
- Users will be informed of any significant access or investigations unless this would compromise safety or legal compliance

8. Use of Images, Videos and Copyrighted Content

Users must not:

- Take or share photographs or videos of students without consent
- Download or use copyrighted images, music, software or materials without permission
- Copy or share school-created materials externally without authorisation

Written permission must be obtained from the copyright holder before use. School staff must also obtain prior approval from a senior leader when using any copyrighted content for presentations, displays, or training.

8. Misuse and Disciplinary Action

- Misuse of school IT systems, including unauthorised access, inappropriate content, breach of data protection, or misuse of email/social media, will be treated as gross misconduct.
- Disciplinary action may include dismissal and/or legal reporting where applicable.

9. Use of Personal Devices (BYOD)

Staff may only use personal devices to access school systems with prior authorisation. Personal devices must:

- Have up-to-date antivirus protection
- Be password-protected
- Not be used to store sensitive school data permanently

If lost or compromised, users must report immediately to the Data Protection Officer.

10. Roles and Responsibilities

Role	Responsibilities
DSL (Designated Safeguarding Lead)	Leads on online safety and manages reports of digital safeguarding concerns
Network Manager	Manages system security, user access and filtering
Headteacher / SLT	Oversees compliance and investigates policy breaches
All Staff and Students	Follow policy expectations and report concerns

11. Breaches of Policy

Breaches of this policy will be investigated and may result in:

- Restricted access to systems
- Disciplinary action in line with staff or pupil/student behaviour policies
- Reporting to external agencies where appropriate

Serious breaches may result in summary dismissal under gross misconduct procedures.

All users are reminded that messages, files or activity logs may be used as evidence in safeguarding or legal investigations.

12. Review and Evaluation

This policy is reviewed annually by the Headteacher and Network Manager in consultation with DSLs and the Data Protection Officer. Updates may also occur following incidents, changes in legislation, or evolving digital risks.