EMAIL, INTERNET AND SOCIAL MEDIA POLICY

1. Introduction

This policy sets out expected standards for the use of email, instant messaging (IM), data storage, internet access and social media by employees, contractors, volunteers and others acting on behalf of the College. It aims to protect learners, staff and the College by establishing clear rules that uphold safeguarding, inclusion, equality and diversity, information security and legal compliance. The policy should be read alongside the Safeguarding Policy, Prevent Policy, Data Protection Policy, Staff Code of Conduct and Disciplinary Policy.

2. Scope

This policy applies to all users granted access to college systems and services, including employees, temporary staff, students, contractors, volunteers and members of the employer forum. It covers use of college-provided or College-managed email, IM, collaboration tools (e.g. Microsoft 365/Teams), data storage, devices and internet access, whether on site or remote. Where staff use personal devices for college business, they must do so only via approved, secure methods as authorised by IT.

3. Acceptable Use

- Make yourself aware of and follow this policy and all related procedures.
- Use College email, IM and internet primarily for business. Personal use must be minimal, outside teaching/learner contact time and must not impact productivity or incur costs.
- Do not access, create, store or transmit material that is illegal, pornographic, sexually explicit, exploitative, hateful, harassing, threatening, incites violence, is discriminatory, or otherwise inappropriate.
- Do not use College systems for private commercial activities or for activities that conflict with the College's interests.
- Do not impersonate others or misrepresent your identity in electronic communications.
- Do not download, install or use unauthorised software, extensions or code. Seek IT approval where unsure.
- Do not attempt to bypass security controls, filtering or monitoring systems.

- Classify and handle information appropriately. Do not disclose confidential information without authority and legitimate purpose.

4. Monitoring, Privacy and Lawful Basis

The College operates proportionate monitoring and filtering to protect users and systems, to meet safeguarding duties and to enforce policy. Communications may be scanned using automated tools to detect malware, data loss risks and prohibited content. Monitoring is conducted in line with UK GDPR and the Data Protection Act 2018 and is overseen by the Data Protection Officer (DPO). Logs may be reviewed by authorised staff where there is reasonable suspicion of misconduct, security risk or safeguarding concern. Where necessary, evidence may be provided to external agencies in accordance with lawful information sharing.

5. Digital Safeguarding and Prevent

- All online activity must support a safe culture. Staff must maintain professional boundaries online and must not use personal accounts to contact learners.
- Staff must immediately report concerns about online harms (e.g. grooming, bullying, exploitation, radicalisation, illegal content) to the DSL through College procedures.
- Filtering and monitoring are maintained to help protect users and identify risks. Staff must not attempt to disable or circumvent these controls.
- Where a safeguarding concern exists, relevant data may be shared with external partners (e.g. children's services, police, Channel/Prevent) when lawful and necessary.

6. Inclusion, Accessibility and Reasonable Adjustments

Digital communication must be accessible and inclusive. The College will provide reasonable adjustments (for example, accessible formats, captions, assistive technology support) so that staff and learners with disabilities or SEND can participate fully. Managers should consider accessibility when selecting tools and planning communications.

7. Equality, Diversity and Belonging Online

- The College complies with the Equality Act 2010 and the Public Sector Equality Duty. Online behaviour must not discriminate, harass or victimise any person, including on the basis of protected characteristics.

- Examples of prohibited content include racist, antisemitic, Islamophobic or otherwise hateful content, homophobic or transphobic abuse, sexist content, disability-based harassment, ageism, and faith-based harassment.
- Online conduct that undermines dignity, creates a hostile environment or damages relationships is unacceptable and may amount to gross misconduct.

8. Email and Instant Messaging Rules

- Use only College-approved email and IM platforms (e.g. Microsoft 365/Teams) for college business.
- Do not auto-forward College email to non-College accounts. Do not configure rules that routinely send content to personal mailboxes.
- Label personal emails as "Personal" where appropriate. Note: such emails may still be accessed under lawful investigation or for continuity.
- Use professional tone and content. Consider your audience and data classification before sending or sharing files/links.
- Use encryption or approved secure methods for sensitive data. Never send special category data via unencrypted channels.

9. Using Social Media

Staff are personally responsible for content they publish online. Even with privacy settings, content may become public. Do not post content that could bring the College into disrepute or that is offensive, disrespectful, discriminatory or breaches confidentiality. Where you refer to your work, make clear you are speaking in a personal capacity and do not represent the College. A disclaimer does not excuse misconduct. Non-approved messaging features within social media apps must not be used for college business.

10. Information Security and Data Protection

- Follow the Data Protection Policy and UK GDPR requirements when processing personal data.
- Store files only in college approved locations. Do not store College data on personal devices or consumer cloud services.
- Use strong passwords and multi-factor authentication where provided.
- Lock screens when away and keep paper records secure. Dispose of confidential waste appropriately.

- Complete mandatory training on data protection, cyber security and online safety at induction and refresh as required.

11. Governance, Risk and Oversight

The Senior Leadership Team has overall accountability for this policy. The DPO, DSL and Head of IT Security provide specialist oversight. A Data Protection Impact Assessment (DPIA) will be completed for new or changed high-risk digital tools or processes (e.g. monitoring platforms, new collaboration tools). Policy effectiveness, incidents and monitoring metrics will be reported annually to drive continuous improvement.

12. Investigations and Disciplinary Action

Potential breaches may be investigated under the Staff Disciplinary Policy. Misconduct may result in sanctions up to and including dismissal. Examples of gross misconduct include accessing or distributing illegal or discriminatory material, serious breaches of safeguarding boundaries, unauthorised disclosure of confidential information, or wilful circumvention of security controls.

13. Guidance and Support

For policy guidance, contact HR. For technical support, contact the IT Help Desk. For safeguarding concerns, contact the DSL. Contact details are available on the College intranet and on safeguarding posters at each site.

14. Legal and Regulatory Framework (summary)

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
- Keeping Children Safe in Education (current edition) and Prevent Duty guidance.
- Online Safety Act 2023 and Ofcom Codes of Practice (as applicable to regulated services).

14.1 Employment law, defamation and intellectual property law as relevant to online conduct.

- Email, instant messaging (IM), data storage and internet facilities are provided primarily for business use. Occasional, reasonable personal use is permitted where it does not interfere with duties or compliance.
- Only College-approved email and messaging services may be used for college business. Do not use personal email or non-approved messaging for college work.
- Employees must not auto-forward College email to non-College accounts. Out-of-Office may be used appropriately.

- Usage of email, IM and internet is monitored lawfully and proportionately for security, compliance and safeguarding purposes. Monitoring may include content scanning in line with our Data Loss Prevention controls.
- Employees are required to provide delegated inbox access to an authorised manager when necessary for continuity or investigation purposes, in line with college procedures.
- Staff must not post content online that is offensive, discriminatory, harassing, defamatory or that brings the College into disrepute. The same standards apply when using personal social media.
- Staff must not communicate with learners via personal accounts or non-approved platforms. Any online safeguarding concerns must be reported immediately to the Designated Safeguarding Lead (DSL).

1. Aims and Implementation

This Policy has been assessed for equality impact by Human Resources.

The purpose of this assessment is to ensure the policy does not unlawfully discriminate against any individual or group and supports the organisation's commitment to equality, diversity and inclusion.

2. Evidence and Data

Barriers could result in		
Equality Group	**Impact**	**Assessment**
Age	Neutral/ Positive	Applies consistently to all age groups. Positive impact through safeguarding measures protecting younger users and learners.
Disability	Positive	Policy explicitly references accessibility, reasonable adjustments, assistive technology and inclusive communication, reducing barriers for disabled users.
Gender Reassignment	Positive	Clear prohibitions on discriminatory, transphobic or abusive content help protect individuals and promote a safe environment.
Marriage and Civil Partnerships	Neutral	No specific impact identified. Policy applies equally regardless of marital status.
Pregnancy and Maternity	Neutral	No adverse impact identified. Policy ensures fair and respectful treatment in all communications.
Race	Positive	Strong protections against racist or discriminatory content and behaviour. Promotes inclusive and respectful online culture.
Religion or Belief	Positive	Policy prohibits faith-based harassment and supports respectful expression, ensuring protection from discrimination.
Sex and Sexual Orientation	Positive	Explicitly prohibits sexist, homophobic or discriminatory behaviour, promoting dignity and inclusion.

3. Assessment of Impact

No adverse impact has been identified. The policy is considered to have a neutral and/or positive impact across protected characteristics.

The policy will be monitored to ensure no disproportionate impact occurs and reviewed if required.

Review Arrangements and Version Control:

This version of The College of Animal Welfare's Email, Internet and Social Media Policy and Procedure replaces all previous versions. This document is subject to regular revision and maintained electronically by its owner. Electronic copies are version controlled. Printed copies are not subject to this control. The College of Animal Welfare will review this policy regularly as part of internal continuous improvement processes and will revise it as and when necessary, in response to changes in our practices, actions from the regulatory authorities or inspections, changes in legislation, or trends identified from previous situations.

Documented changes from previous version	
Section	New document
All document	Updated information
Equality Impact Assessment	New section