ACCEPTABLE USE POLICY - WORKFORCE

for adoption by all CDAT schools

This policy is informed by the Christian values which are the basis for all of CDAT's work and any actions taken under this policy will reflect this.

'Blessed are those who act justly, who always do what is right'

Psalm 106:3

Approved by	Date	Review Schedule	Date of next review
Audit and Risk Committee	December 2025	Every two years	December 2027

The document governs our workforce's use of the corporate network and cloud-based systems, including when authorised to use personal devices.

Email, Instant Messaging, and Internet Use

We provide the workforce with email accounts, instant messaging (IM) functionality, and Internet access to assist with performing their duties. For the benefit of doubt, Instant Messages are classed as email communications in this policy.

Personal Use

Whilst email accounts, IM, and the Internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Use must not tarnish our reputation or infringe on business functions
- Emails sent to and from corporate accounts are our property
- We may monitor the use of accounts and systems and access any personal messages and browsing history contained within
- Emails sent to or from their email account may be disclosed under Freedom of Information and/or Data Protection Legislation
- We reserve the right to cleanse email accounts at regular intervals, which could result in personal emails being erased from the corporate network
- We reserve the right to suspend access to accounts and systems anytime.

Inappropriate Use

We do not permit users to send, forward, or solicit emails, or use the Internet in any way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic messages, images, cartoons, jokes, or movie files
- Unwelcome propositions, profanity, obscenity, slander, or libel
- Any messages or content containing ethnic, religious, political, or racial slurs
- Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Users are also not permitted to use the Internet in a way that could affect others' usage. This means not streaming or downloading media files and not using the Internet to play online games.

Other Business Use

Users are not permitted to use emails or the Internet to carry out their own business or the business of others. This includes, but is not limited to, work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.

Security

Users will only use corporate accounts and systems in accordance with our Information Security Policy. In particular, users will not:

- Click on links from untrusted or unverified sources
- Use insecure email transmission methods when sending personal data
- Sign up for marketing material that could jeopardise our IT network
- Send excessively large email attachments without prior authorisation from the SIRO and/or our IT Provider
- Attempt to download any software onto corporate devices. This can present a virus risk and/or breach of software license requirements.

Group Email Accounts

Users may be permitted to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity, and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to the suspension of a user's email rights.

The SPOC will be responsible for allowing access to group email accounts. All email traffic to and from individual and group accounts may be monitored.

Social Media and Private Messaging Apps

We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. However, we also recognise that social media poses a data protection risk due to its open nature and capacity to broadcast to many people quickly.

Corporate Accounts

We may have social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about our business activities. Authorised users will be given the usernames and passwords to these accounts, which must not be disclosed to any other user within or external to the organisation. The SPOC will be responsible for allowing access to corporate social media accounts.

Corporate social media accounts must not be used to disseminate personal data in an open forum or by direct message. Doing so would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

- Tarnish our reputation
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs
- Be construed as sexually explicit
- Be construed as political beliefs or commentary.

Personal Accounts

We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

- During working hours
- Using corporate equipment
- To conduct corporate business

- To contact or approach our clients, customers, or partners
- Make posts that relate to us or refer to information gained through your role within the organisation
- Identify your role within our organisation.

Private Messaging Apps

Social messaging apps such as WhatsApp, Facebook Messenger, etc. must not be used for communicating any school or Trust business. Information held in non-corporate communication channels may be subject to FOIA if it relates to official business.

Telephone and Video Conferencing Use

We provide users access to telephone and video conferencing services to assist with communication and performing their duties.

Personal Use

Whilst telephone and video conferencing services should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Usage must not tarnish our reputation or infringe on business functions
- We may monitor and access call history and recordings
- We reserve the right to suspend telephone and video conferencing usage at any time
- Telephone calls, video conference recordings, or transcripts may be disclosed under the Freedom of Information and/or Data Protection Legislation.

Inappropriate Use

We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use these services to carry out their own business or the business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.