Darlinghurst
ACADEMY

ICT Acceptable Use

December 2025

Date created	December 2025
Version	1
Status	Ratified
Applicable to	All staff
Author	ALS
Checked by	LGB
Valid from	December 2025
Review date	December 2027

1. Network access and use

Darlinghurst Academy provides ICT equipment and systems to support learning, communication, and Academy operations, including access to cloud services such as Microsoft 365 and Bromcom MIS. All users must follow this Acceptable Use Policy whenever accessing Academy ICT or data.

1.1 Unacceptable use

The following are not permitted:

- Sending, displaying, or storing obscene, offensive, discriminatory, or explicit material.
- Intentionally accessing illegal, hateful, extremist, or otherwise inappropriate content.
- Harassing, threatening, or bullying others using ICT.
- Installing unauthorised software or altering Academy devices without permission.
- Damaging equipment, introducing malware, or wasting ICT resources.
- Violating copyright or licensing laws.
- Using another person's credentials or accessing their files without permission.
- Disclosing personal or confidential Academy information without authority.
- Using personal devices to capture unauthorised images or recordings.
- Using Academy ICT for commercial purposes or personal profit.
- Attempting to bypass filtering, security, or monitoring systems.

Breaches may lead to withdrawal of access, disciplinary action, and/or referral to external agencies.

1.2 The Academy will:

- Provide filtering, monitoring, and anti-malware protection on Academy systems.
- Monitor ICT usage for safeguarding, security, and compliance.
- Provide users with internet safety and cyber awareness guidance.
- Review ICT security controls regularly to align with best practice.

2. Mobile phones and smart devices

These rules apply to children, staff, volunteers, parents, and visitors.

2.1 Students

- mobile phones/smart devices are not permitted for use on site unless specifically authorised for safeguarding or medical reasons.

- Devices used without permission may be confiscated and collected by a parent/carer.
- Children must not record staff or other children without explicit permission.
- **Exams:** Mobile devices must not be taken into any examination. Any breach will be reported to the examination board and may lead to disqualification.

2.2 Staff – personal devices

- Staff bring personal devices at their own risk; the Academy accepts no liability for loss/damage.
- Personal devices must be kept updated with security patches.
- Sensitive Academy data must not be stored permanently on personal devices.
- Microsoft 365/Bromcom apps may only be used on personal devices using Academy credentials; personal email addresses must not be used for Academy business.
- The Academy may revoke access if a device is insecure or in breach of policy.

2.3 Staff – Academy-issued devices

- Academy devices are for business use and must remain under staff control.
- Devices must be protected by passcode and encryption, and kept updated.
- Photographs of pupils must only be taken on Academy-issued devices and stored on approved Academy platforms.

2.4 Parents and visitors

- Filming/photography on site is not permitted unless authorised by SLT.
- Visitor internet access, where provided, is filtered and monitored and must follow this policy.

3. Email use

- Staff mailboxes are for Academy business only.
- Personal email accounts must not be used for Academy communications.
- All Academy email is subject to monitoring for safeguarding, security, and compliance.
- Suspicious emails, links, or attachments must be reported immediately to Trust IT.

Mailbox investigations may only be undertaken with CEO authorisation and with an audit trail.

4. Taking photographs and use of cameras

- Pupil photo consent procedures apply to all Academy photography.
- Staff must not use personal phones to photograph/record pupils.
- Images must be stored securely on Academy systems and deleted from devices promptly.
- Images must not be taken in toilets, changing areas, or medical rooms.

5. Volunteers and trainees

Volunteers and trainees using ICT equipment must follow this policy and complete mandatory safeguarding/data protection training before access is granted.

6. Breach of policy

Failure to follow this Acceptable Use Policy may result in withdrawal of ICT access, disciplinary action, and/or referral to external agencies where required.