Tarbiyyah Global Academy
Part of the Tarbiyyah Education Trust · globalacademy.tarbiyyah.co.uk · globalacademy@tarbiyyah.co.uk · 020 3719 8697

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Safe, responsible use of Academy platforms, devices and the internet

ACADEMIC YEAR 2026 – 2027

Policy name	Online Safety and Acceptable Use Policy 2026–2027
Applies to	All pupils, parents, staff, trustees and volunteers of Tarbiyyah Global Academy
Policy owner	Designated Safeguarding Lead and Digital Lead
Approved by	Ustadh Abu Zayn Haneef Sandhar, Headteacher
Agreed with	The Chair of Trustees, Tarbiyyah Education Trust
Date of issue	1 September 2026 (version 1.3)
Next review due by	31 August 2027
Basis	New policy for online provision
Read alongside	Child Protection and Safeguarding Policy; Live Lesson Protocols; Recording of Live Lessons and Use of Images Policy; Behaviour and Online Conduct Policy; Data Protection Policy; Technology and Digital Wellbeing guidance within the Health, Safety and Wellbeing Policy
Availability	Published on the Academy website and Parent Portal. Available in large print or another accessible format on request.

CONTENTS

1. Purpose
2. Scope
3. Our Approach: the Four Cs
4. How the Academy Secures its Platforms
5. Acceptable Use — Pupils
6. Acceptable Use — Parents
7. Acceptable Use — Staff
8. Teaching Online Safety
9. Artificial Intelligence
10. Responding to Incidents
11. Monitoring and Review
Appendix A — Pupil Acceptable Use Agreement (summary for signature)

1. Purpose

Tarbiyyah Global Academy exists online. Our classrooms, corridors and noticeboards are digital, so online safety is not a topic taught once a year; it is the environment in which every lesson happens. This policy explains how the Academy keeps its platforms safe, what we expect of pupils, parents and staff, and what happens when things go wrong.

2. Scope

This policy applies to every person who uses Academy systems, and to every Academy system, including:

- the Academy's live-lesson platform (currently Microsoft Teams), joined from the Student Portal (live lessons; assignments and quizzes are in the Student Portal);
- the Academy Parent Portal, Student Portal and staff area;
- Academy email accounts and calendars;
- approved learning subscriptions issued by the Academy. It also applies to conduct outside Academy systems where that conduct affects the safety or wellbeing of a member of the Academy community.

3. Our Approach: the Four Cs

Following KCSIE, we plan online safety around four areas of risk:

Area	Examples
Content	Exposure to illegal, harmful or inappropriate material, misinformation, extremist content, pornography, self-harm content
Contact	Harmful interaction with other users, including grooming, sextortion, and adults posing as children
Conduct	A pupil's own behaviour that increases risk or causes harm, such as sharing images, cyberbullying or oversharing personal information
Commerce	Online gambling, scams, phishing, inappropriate advertising and financial exploitation

4. How the Academy Secures its Platforms

- **Academy accounts only.** Pupils and staff use Academy-issued accounts. Personal accounts are never used for teaching or contact with pupils.
- **Controlled meetings.** Only staff can create live lessons. The lobby is enabled so that only Academy accounts are admitted; anonymous or external participants cannot join.
- **Restricted pupil permissions.** Pupils cannot present, record, start meetings, create breakout rooms or remove others. Private pupil-to-pupil chat is disabled; lesson chat is visible to staff and retained.
- **Recording.** Live lessons are recorded for safeguarding and quality assurance in line with the Recording of Live Lessons and Use of Images Policy.
- **Single sign-on and multi-factor authentication** for staff accounts; access is revoked immediately when a device is lost or a staff member leaves.
- **Secure assessments** are released through the Student Portal only to the pupil's class during the test window, and are sat under live invigilation with cameras on, as set out in the Academic Integrity and Secure Assessment Policy.
- **Audit logs.** The Digital Lead reviews the portal audit log and the platforms' sign-in and activity logs every month, and straight away when a concern is raised (see below).

The Digital Lead

The Digital Lead is the member of staff the Headteacher names to look after the security of Academy systems (currently: [name to be confirmed]). The Digital Lead:

- reviews the audit logs every month, looking at a sample of activity and at anything unusual, such as sign-ins from unexpected places, changes to accounts or permissions, records opened in bulk, and safeguarding or message records opened;
- passes anything that suggests a safeguarding risk to the DSL, and anything that suggests a data breach to the Data Protection Officer, on the same day;
- manages accounts and access: new starters, leavers, lost devices and password resets;
- checks platform settings each term (lobby, pupil permissions, chat and recording);
- keeps a short record of each review and what was done, and reports to the DSL each term and to trustees each year.

The Digital Lead looks at pupils' messages or records only as part of a review agreed with the DSL, and their own access is recorded in the audit log like everyone else's.

> **Filtering at home**
>
> The Academy does not control the internet connection in a pupil's home, so we offer every family help to set up:
>
> - **router-level filtering:** most broadband providers offer a free family filter that blocks harmful and adult sites on every device in the home. It is switched on in the provider's account or app, or in the router's settings;
> - **device parental controls:** for example Microsoft Family Safety on Windows, Screen Time on iPad and Mac, and Google Family Link on Android and Chromebook, to filter websites, limit apps and set screen-time limits;
> - **safe search and restricted modes** in search engines and video sites;
> - **devices in shared family spaces** for younger pupils, and phones and tablets charged outside bedrooms overnight.
>
> The guidance is on the Safeguarding page of the Academy website and is covered in the parents' induction session, and any family can ask the Digital Lead for help to set it up.

5. Acceptable Use — Pupils

Every pupil (with a parent for pupils in Years 1 to 6) agrees to the Pupil Acceptable Use Agreement at enrolment. In summary, pupils will:

- use only their own Academy account and keep their password private;
- join lessons from a quiet, appropriate space, with their camera on unless the teacher agrees otherwise;
- be kind and respectful in chat, voice and work, and never share hurtful, rude or unsafe content;
- never record, photograph or screenshot a lesson, a teacher or another pupil;
- never share lesson links, codes or Academy materials with anyone outside the Academy;
- never share personal information such as addresses, phone numbers or social media accounts with other pupils in lessons;
- keep mobile phones and other devices away during lessons unless the teacher asks for them;
- tell a teacher, their form tutor or the DSL straight away if they see or receive something that worries them. Breaches are managed under the Behaviour and Online Conduct Policy. Anything that suggests a pupil is at risk is managed under the Child Protection and Safeguarding Policy.

6. Acceptable Use — Parents

Parents support safe learning at home by:

- providing a suitable device, a reliable connection and a quiet, appropriate study space, with a tablet with a stylus (recommended) or, without one, access to printing (at home, at a local library or similar) for worksheets and the lesson PDF;
- supervising younger children's device use and applying parental controls;
- never recording, sharing or posting lessons or images of staff or other pupils;
- keeping out of camera view and not intervening during live lessons, except to support their own child or in an emergency;
- raising concerns through the proper channels set out in the Parent Communication Charter, rather than through public posts or group chats.

7. Acceptable Use — Staff

Staff will:

- use Academy accounts and approved platforms only, and never contact pupils through personal phones, personal email or social media;
- never hold unrecorded one-to-one video calls with a pupil. Where one-to-one support is needed, the call is scheduled through Academy systems, recorded, and the parent is informed;
- teach from a neutral, professional background with no personal information visible, dressed appropriately;
- lock or end meetings correctly so that pupils cannot remain in an unsupervised meeting;
- protect personal data, lock devices when unattended, and report lost devices or suspected breaches immediately;
- report any online safety concern to the DSL on the same day. Full expectations are set out in the Live Lesson Protocols.

8. Teaching Online Safety

Online safety is taught through PSHE, Computing and Islamic Studies, and reinforced in assemblies and form time. The curriculum is age-appropriate and includes: recognising reliable information and misinformation; privacy and digital footprints; healthy online relationships and boundaries, modesty and protection from exploitation; recognising grooming and manipulation; managing screen time; artificial intelligence and deepfakes; and how to report. Islamic Studies connects online conduct with adab, guarding the tongue, and the amanah of what we see and share.

9. Artificial Intelligence

Pupils may use AI tools only where a teacher has permitted it for a specific task, and must declare how they used it. Using AI to complete assessed work without permission is academic misconduct under the Academic Integrity and Secure Assessment Policy. Staff will not enter pupils' personal data into AI tools that are not approved by the Academy, and will be alert to AI-generated images being used to bully or exploit.

10. Responding to Incidents

Incident	Response
Upsetting or inappropriate content seen by a pupil	Reassure, record, inform the DSL, contact parents, review platform settings
Cyberbullying between pupils	Anti-Bullying and Cyberbullying Policy; preserve evidence; support both pupils
Suspected grooming or contact from an unknown adult	Do not alert the adult; secure evidence; DSL refers to police/CEOP and children's social care
Nudes or semi-nudes shared	Do not view or forward; DSL follows UKCIS guidance
Unauthorised person joins a lesson	Remove, lock the meeting, report to the DSL and Digital Lead, review access logs
Compromised account or data breach	Revoke access, reset credentials, inform the Data Protection Officer within 24 hours

11. Monitoring and Review

The DSL and Digital Lead review this policy annually, together with platform settings and incident logs, and report to trustees. The policy is also reviewed after any significant online safety incident or change of platform.

Appendix A — Pupil Acceptable Use Agreement (summary for signature)

I will…	I will not…
Use only my own Academy account	Share my password or lesson links
Keep my camera on and be ready to learn	Record, screenshot or photograph lessons
Be kind in chat and in my words	Post anything hurtful, rude or unsafe
Tell a trusted adult if something worries me	Give personal details to people online
Keep my phone away during lessons	Open other apps or websites during lessons

Pupil name: _____ Signature: _____ Date: _____ Parent name: _____ Signature: _____ Date: _____

Approved by: Ustadh Abu Zayn Haneef Sandhar, Headteacher · Next review due: 31 August 2027 · Tarbiyyah Global Academy · A specialist education, rooted in faith