



A product of



ClassPilot Acceptable Use Policy

Version 0.2 | 19 September 2026

These rules explain how to use ClassPilot safely for school assessment and reporting. Schools should give this policy to staff before access is granted. It supports, and does not replace, school safeguarding, information-security and data-protection rules.

1 Authorised school use

Use ClassPilot only for your authorised school duties and within your assigned school, role and class permissions. Access is for school-authorised staff, not for pupils or parents to use directly. Do not share an account, let someone work under your identity or use a former colleague's account.

The school must keep user permissions current and remove access when staff leave or their duties change. A subscription covers only the schools and user entitlement stated in its Order Form; it does not automatically allow access across a trust.

2 Protect accounts and devices

- Use your own authorised work account and keep passwords, sign-in codes and recovery details private. Use multifactor authentication wherever it is provided or required by your school.
- Use a device and network permitted by your school, keep software updated, lock the screen when unattended and sign out of shared devices.
- Check unexpected invitations and links before opening them. Never send passwords, one-time codes or credentials to support.
- Tell your school administrator and support@edapt-tech.co.uk promptly if you suspect an account is compromised or permissions are incorrect.

3 Enter only necessary and accurate information

Check that data belongs to the correct school, pupil, class and academic year. Use only the approved import fields and relevant educational content. The standard dataset does not require date of birth, home addresses, parent contact details, attendance history or safeguarding records.

Do not place unnecessary health information, protected characteristics or family circumstances in comments. Where relevant SEN or other sensitive educational information is needed, follow your school's instructions and restrict it to the purpose and users who need it.

4 Review reports and use AI responsibly

Check assessment information and report content before approval, export or sharing. Follow the ClassPilot AI Information and Responsible Use Guide when using AI-assisted drafting. AI suggestions may be inaccurate or biased and must not substitute for professional judgement.

Do not use ClassPilot AI to diagnose a condition, decide safeguarding action, allocate support or make another significant decision about a pupil. Do not transfer pupil records into a separate public AI service or unapproved tool.

5 Handle exports and support requests safely

Download and share information only through school-approved routes with authorised recipients. Confirm the correct pupil and recipient before distributing a report. Protect exported files and delete unnecessary local copies under school policy.

Use fictional examples or redacted screenshots in support requests wherever possible. Do not email pupil spreadsheets or unredacted reports unless a secure method and the necessary scope have been agreed with us.

6 Prohibited activity

- Accessing another school's data, bypassing permissions, impersonating users or concealing unauthorised activity.
- Uploading malicious code, interfering with availability, or attempting intrusive testing without prior written authorisation.
- Unapproved automated extraction, account sharing, resale, or copying of the service beyond the permissions in the agreement or applicable law.
- Entering unlawful, abusive or discriminatory content, deliberately falsifying records, or using data for advertising or unrelated personal purposes.

7 Report concerns and respond to restrictions

If you unexpectedly see another school's or an unauthorised pupil's data, stop viewing it. Do not explore, download or forward it. Report the time, page and a minimal description to your school administrator and support@edapt-tech.co.uk using the subject Urgent Security Incident.

We may restrict affected access where reasonably necessary to protect people, data or the service, following the Service Terms. We will investigate and work with the school on corrective action. Schools remain responsible for their own staff conduct processes. For an immediate safeguarding emergency, use the school's safeguarding procedure and emergency services where appropriate; support is not an emergency service.