

Acceptable Use Policy

Acceptable Use Policy (AUP)

Policy	Acceptable Use Policy (AUP)
Version	1.0
Effective date	2 October 2026
Status	Incorporated by clause 16 of the Standard Terms of the Platform Licence Agreement
Address	vhire.com/legal/acceptable-use

Talgrid Tech Private Limited, trading as NextGeek and vHire (**Talgrid**).

This is a Policy under clause 16 of the Standard Terms. It is the AUP that clause 2.5 refers to and it ranks under clause 1.3(e). It has no governing-law or dispute clause of its own; clauses 13 and 15 of the Standard Terms apply. Terms not defined here have the meaning given in the Standard Terms.

This AUP applies to the Customer and to every Authorised User, which includes the Customer's clients, interview panellists and vendors whom the Customer's administrator permits to use its account (clause 2.4). The Customer is responsible for their acts and omissions as if they were its own.

1. Account and access

The Customer and its Authorised Users shall not:

- (a) share login credentials, or allow access by anyone who is not an Authorised User;
- (b) use one user licence for more than one person, or pass a user licence between people in order to avoid buying more. Under a Per-User Licence each user licence is held by one named Authorised User at a time, and may be reassigned when its holder no longer needs access (clause 2.1). Credentials are never shared under any licence. An Enterprise Platform Licence has no cap on the number of Authorised Users;
- (c) get round, or try to get round, a limit on the number of user licences, an allowance of Usage Units, or a rate limit; or
- (d) access the Platform other than through the interfaces Talgrid provides.

2. Platform integrity

The Customer and its Authorised Users shall not:

- (a) reverse engineer, decompile or try to derive the source code, models or underlying algorithms of the Platform;
- (b) scrape, crawl or bulk-extract data, other than through documented APIs and within documented rate limits;
- (c) probe, scan or test the vulnerability of the Platform, or breach or try to breach its security, except under a written authorisation from Talgrid;
- (d) introduce malware, or interfere with the operation of the Platform for other customers; or
- (e) use the Platform to build, or help a third party to build, a competing product or service.

3. Assessment integrity

- (a) Assessment questions, blueprints, scoring logic and adaptive selection are Talgrid's confidential information under clause 10.2.
- (b) The Customer shall not copy, export, publish or disclose them, or allow a candidate to keep them.
- (c) The Customer shall not administer an Assessment in a way designed to reveal the question bank.

Disclosure compromises the integrity of an Assessment for every customer on the Platform, not only the one that discloses.

4. Candidate data and communication

The Customer shall:

- (a) have a lawful basis for all data it uploads or instructs Talgrid to process, including any notice or consent its law requires;
- (b) have a lawful basis to contact candidates through any channel it enables, in line with the law on calls, messages and consent. That includes the rules of the Telecom Regulatory Authority of India and the Do Not Disturb register, WhatsApp's opt-in requirements, and, for personal data, the notice and consent that the Data Protection Laws require before outreach;
- (c) not upload data obtained in breach of another party's terms, including a job board's limits on seats, downloads and database use; and
- (d) not use the Platform to send unsolicited bulk communication that is unrelated to a genuine recruitment purpose.

5. Revealed data (clause 7.1)

This section applies once Reveal is available to the Customer (DPA, section 2.8). The Customer shall not:

- (a) resell, or share outside its organisation, a record delivered on a Reveal. The one exception is that a Customer recorded in its Order Form as a staffing provider may share a record with a client for whom it is searching;
- (b) bulk-export revealed data. The one exception is the export on exit under clause 6.6;
- (c) build a database from revealed data. Keeping a revealed record in the Customer's own applicant tracking system and using it for recruitment, as clause 7.1 provides, is not building a database; or
- (d) fail, within seven (7) days of a withdrawal notice, to delete a candidate's revealed record or to stop processing it, unless the Customer holds the record on another lawful ground that does not depend on the Reveal or the law requires it to keep it (clause 6.5).

6. Minors, notice and consent

The Customer shall not:

- (a) upload personal data of anyone under eighteen;
- (b) enable proctoring, recording or other monitoring of anyone under eighteen;
- (c) use recording, proctoring or verification except with the notice and consent the law requires, including what sections 13.1, 13.4 and 15.1(g) of the DPA and, once published, the Service Terms describe; or
- (d) try to re-identify de-identified data.

7. Hiring conduct

The Customer shall not use the Platform:

- (a) to screen, rank or reject candidates on any characteristic the law protects;
- (b) to use an automated output as the sole basis for rejecting a candidate (clause 7.2);
- (c) to use AI Interview or Assessment outputs to infer a candidate's emotions, health or a characteristic the law protects;
- (d) to advertise a role that does not exist, or to collect candidate data without a genuine hiring purpose;
- (e) to require a candidate to pay a fee; or
- (f) to process a government identity document except where an Assessment or verification requires it, or to copy or keep one outside the Platform.

8. Prohibited content

Customer Data shall not be unlawful, defamatory or obscene, and shall not infringe another party's intellectual property or privacy rights.

9. Enforcement

9.1 Talgrid may investigate a suspected breach of this AUP, and may suspend the affected function, Authorised User or account under clause 2.6.

9.2 Talgrid gives notice before it suspends, except where an immediate security risk makes prior notice impracticable (clause 2.6). Fees continue to accrue during a suspension, as clause 2.6 provides.

9.3 A material breach of this AUP is a material breach of the Agreement. The cure period in clause 5.3 applies.

10. Changes

This AUP changes under clause 16.2 of the Standard Terms.