Desian Recruitment Ltd - Policy Management, Review & Control Policy

This policy defines how organisational policies are created, approved, reviewed, updated, controlled and communicated to the agency staff, candidates and clients.
It ensures all policies remain legally compliant, operationally effective and audit-ready and it applies to all organisational policies.

Policies must reflect current legislation, regulatory guidance, and best practice, with only the latest approved versions being used. All policies must be easily accessible to all relevant staff, and all changes must be documented and traceable.
Policies will be updated when new legislation or regulations are introduced, a compliance gap is identified or where a new service / risk area emerges.
These updated or new policies will align with legal and regulatory requirements and will have approval before implementation.

Policy Approval, Inclusion and Maintenance

All policies must be formally approved before release by.

- Senior Management / Directors
- Compliance Officer / DPO (where applicable)
- Safeguarding Lead (for safeguarding policies)
- No policy may be issued without approval.

Each policy must include:

- Version number
- Date of issue
- Review date
- Policy owner / Approver
- Approval sign-off
- Version Format Example:
- v1.0 – Initial release
- v1.1 – Minor update
- v2.0 – Major revision

A Policy Register must be maintained containing:

- All current policies
- Version history
- Review dates
- Responsible owners

Policies must be reviewed annually or immediately following legislative changes, safeguarding updates, audit findings or serious incidents / complaints.
Reviews will include legal compliance checks, operational effectiveness risk assessment and feedback from staff.

Policy updates may be:

Minor Updates
Typographical corrections
Clarifications
Non-material changes
Major Updates
Legal/regulatory changes
Process changes
Safeguarding updates
All updates must:
Be documented in version history
Be approved before release

Policy Communication

All staff must be informed of new policies, updates and key procedural changes by either email notifications, staff meetings, via training sessions or accessible via internal systems. Critical policies (e.g. safeguarding, data protection) must include mandatory staff acknowledgement.

Staff Acknowledgement & Training

Confirm they have read and understood policies
Complete training where required
Mandatory areas:
Safeguarding (KCSIE)
Data protection (GDPR)
Records of acknowledgement must be retained for audit purposes.

Policies must be stored in a centralised, controlled location
With restricted editing access and read access for relevant staff.

Policy Withdrawal / Archiving

When a policy is replaced or no longer valid:
It must be clearly marked “Superseded”, removed from active use and securely archived.
Retain for 6 years for Audit purposes

Roles & Responsibilities

Policy Owner

Maintains and reviews policy
Ensures compliance

Compliance Manager / DPO

Reviews legal and regulatory alignment
Supports audits

Safeguarding Lead (DSL)

Oversees safeguarding-related policies
Ensures KCSIE compliance

Senior Management

Approves policies
Ensures organisational compliance

Staff

Follow policies
Complete required training
Report issues or gaps

Desian will conduct regular policy audits, track review deadlines, analyse incidents / complaints and update policies based on lessons learned.

Failure to follow this policy may result in disciplinary action, audit failure and legal or regulatory penalties.

Approved by: Andrew Wainwright
Position: Operations Director
Effective Date: 01/05/26
Next Review Date: 01/05/27