Policy Pack

Policy Contents

1. Complaints Handling Policy

Purpose

To ensure that all complaints, whether internal or external, are handled promptly, fairly, and constructively.

Scope

Applies to all directors, partners, clients, and members of the public who engage with Allegr Ltd.

Policy Statement

Allegr Ltd is committed to maintaining high standards in all aspects of its operations. Any complaints received will be taken seriously, acknowledged promptly, and resolved wherever possible at the point of origin.

Procedure

1. Internal complaints should be submitted in writing to the Board via email. External or public complaints should be submitted in writing through the website. Digital platform complaints can be submitted through the platform's Pinboard Contact function or using the 'Flag' tool for reporting issues on content, groups and chat.
2. Acknowledgement will be sent within 3 working days.
3. A Director will investigate and respond within 10 working days.
4. If further investigation is needed, an update will be provided with a revised timeframe.
5. All complaints and resolutions will be documented and reviewed annually.

The public complaints procedure can be found on the website and the policy will be annually reviewed and updated if required:

www.militaryapp.org/policies/complaints-and-feedback

2. Conflicts of Interest Policy

Purpose

To ensure transparency and prevent decisions being influenced by personal interests.

Scope

Applies to all directors and any contracted partners or advisors.

Policy Statement

All parties involved in Allegr Ltd must disclose any actual or potential conflicts of interest. A conflict may arise when personal interests could interfere with professional duties.

Procedure

1. Disclose any potential conflict to the Board as soon as it arises.
2. The Board will determine if the interest requires action, such as recusal from decisions.
3. All conflicts and resolutions will be recorded in a Conflict of Interest Register.

3. Risk Management Policy

Purpose

To identify, assess, and manage risks in a proportionate and proactive manner.

Scope

Applies to all activities undertaken by Allegr Ltd.

Policy Statement

Allegr Ltd is committed to maintaining a simple and effective approach to identifying and mitigating business risks, including reputational, operational, legal, and data-related risks.

Procedure

1. Risks are discussed during bi-annual director meetings and quarterly during operational meetings.
2. Identified risks are logged and assessed based on likelihood and impact.

3. Mitigation actions are assigned and reviewed.
4. Serious or emerging risks are escalated immediately to the full board.

Armed Forces Third Party Assurance

With specific reference to Allegr Ltd activities with the Military App and Armed Forces Community, there is an identified need to consider the suitability and credibility of third party providers - in particular when considering the provision of: support and professional services to app members; Information, Advice and Guidance; community management and content moderation.

To deliver assurance across the Military App platform, all Community Clients that sign the platform's Subscription Agreement must be a registered members of COBSEO (The Confederation of Service Charities) to ensure consistency and best practice. In the event of a new potential Community Client not being a COBSEO member, Allegr Ltd Senior Management will seek appropriate sector advice.

For governance considerations on Third Party Assurance, refer to Governance Framework, Section 8.

---

4. Safeguarding Adults Policy

Allegr Ltd's Safeguarding Adults Policy can be found on our website:
www.militaryapp.org/policies/safeguarding-adults-policy

The Code of Conduct (Section5) can be found on our website:
www.militaryapp.org/policies/safeguarding-code-of-conduct

Purpose

Allegr Ltd is committed to safeguarding adults and promoting their wellbeing in all aspects of our work. This policy sets out how we prevent harm, respond to safeguarding concerns, and uphold safe practice across our digital community platform and related activities.

Scope

This policy applies to:

- Directors, contractors, and anyone working on behalf of Allegr Ltd
- Adults who engage with or are affected by our services and digital platform
- Partner organisations, community clients, and groups using the platform, insofar as safeguarding responsibilities intersect

Allegr Ltd’s platform is **not intended for children**, and users must be aged 18 or over.

Policy Statement

Allegr Ltd recognises its responsibility to take all reasonable steps to safeguard adults who may be at risk of harm, abuse, neglect, or exploitation.

We operate a digital community platform serving the UK Armed Forces community. While our community clients (all registered charities) are responsible for moderating their own community content and activities, we are committed to:

- Providing a safe digital environment
- Enabling effective reporting and escalation of safeguarding concerns
- Working collaboratively with partners and external agencies where safeguarding issues arise

We have a **zero-tolerance approach** to abuse and are committed to acting promptly, proportionately, and transparently when concerns are raised.

Definitions

An *adult at risk* is a person aged 18 or over who:

- Has needs for care and support, and
- Is experiencing, or is at risk of, abuse or neglect, and
- Is unable to protect themselves because of those needs

Abuse may include, but is not limited to: physical, emotional, sexual, financial, discriminatory abuse, neglect, coercive control, or online harm.

Roles and Responsibilities

- **Safeguarding Lead:**
  Rachel Mitchell (Director)
  Email: rach@allegr.org
  Tel: +44 7779 323220

The Safeguarding Lead is responsible for:

- Receiving and assessing safeguarding concerns
- Ensuring appropriate action and escalation
- Liaising with external agencies where required
- Maintaining secure safeguarding records

All directors, contractors, and partners are responsible for:

- Being alert to safeguarding concerns
- Acting in line with this policy
- Reporting concerns promptly

Safeguarding in a Digital Community Setting

Allegr Ltd recognises the specific risks associated with online and community-based environments. We address these by:

- Providing platform tools to report concerns, inappropriate behaviour, or harmful content
- Supporting community clients in managing and moderating their own spaces
- Ensuring that Armed Forces community clients are COBSEO members guided by best practice
- Escalating safeguarding concerns that present risk of harm beyond routine moderation
- Taking appropriate action where platform terms or safeguarding standards are breached

Small, localised activity groups (such as walk-and-talks or coffee clubs) supported via the platform are required to follow the specific safeguarding policies and procedures provided to each walk leader or group admin.

Reporting Safeguarding Concerns

Safeguarding concerns may be raised by:

- Platform users.
- Community clients or group organisers.
- Contractors or members of the public

Concerns should be reported as soon as possible to the Safeguarding Lead using:

- Direct contact (email or phone), or
- The platform's reporting or contact mechanisms. These include: The Pinboard Contact function; The 'FLAG' tool embedded within app new or support articles, events, groups and chat.

All reports will be treated seriously and handled confidentially, in line with data protection requirements.

Responding to Concerns

When a safeguarding concern is raised, Allegr Ltd will:

1. Listen carefully and take the concern seriously
2. Assess the level of risk and urgency
3. Take appropriate action to reduce harm
4. Refer to statutory services (such as adult social care or the police) where necessary
5. Keep clear, secure records of concerns and actions taken

Allegr Ltd will not investigate safeguarding matters beyond its remit but will support appropriate referral and cooperation with relevant authorities.

External Advice and Support

For independent safeguarding advice, individuals may also contact:

Ann Craft Trust
Tel: 0115 951 5400
Email: Ann-Craft-Trust@nottingham.ac.uk
Website: www.anncrafttrust.org

Review and Governance

This policy is approved by the Board and is reviewed annually, or sooner if:

- There are changes in legislation or guidance
- A significant safeguarding incident occurs
- Operational changes require review

DBS Checks

Directors are to provide a record of DBS checks, maintaining validing every 2 years. New consultants or contractors are to provide a recent DBS certificate (within 6 months) and depending on the role and any community engagement fulful any further checks or requirements set by Directors.

---

5. Safeguarding Code of Conduct

The Safeguarding Code of Conduct can be found on our website, including a sign-off form for contractors, partners, community clients and selected group admins: www.militaryapp.org/policies/safeguarding-code-of-conduct

Purpose

This Code of Conduct sets out the standards of behaviour expected of everyone working for, representing, or engaging with Allegr Ltd. It supports our commitment to safeguarding adults, promoting respect, and maintaining a safe and inclusive digital community.

Scope

This Code applies to:

- Directors, contractors, consultants, and anyone acting on behalf of Allegr Ltd
- Partner organisations and community clients using the platform
- Group organisers and facilitators of activities supported through the platform

Expected Standards of Behaviour

All individuals covered by this Code must:

- Treat others with dignity, respect, and fairness at all times
- Act in a way that upholds trust, integrity, and professionalism
- Be mindful of power imbalances and avoid behaviour that could be perceived as intimidating, coercive, or inappropriate
- Communicate respectfully in all online and offline interactions

Professional Boundaries

Those representing Allegr Ltd must:

- Maintain appropriate boundaries in digital and community interactions
- Avoid forming inappropriate or exclusive relationships with platform users or beneficiaries
- Not use their role to seek personal, financial, or emotional gain
- Avoid private communications that could place themselves or others at risk

Online Conduct

When using the Allegr Ltd platform or related digital spaces, individuals must:

- Use the platform responsibly and in line with its terms of use
- Not engage in harassment, bullying, discrimination, or harmful behaviour
- Not share offensive, abusive, or inappropriate content
- Respect confidentiality and privacy at all times

Safeguarding Responsibilities

Everyone has a responsibility to be alert to safeguarding concerns and to report them promptly in line with Allegr Ltd's Safeguarding Adults Policy

- Safeguarding concerns must not be ignored, minimised, or investigated independently
- Allegations or concerns will be handled confidentially and appropriately

Compliance and Breaches

Failure to follow this Code may result in action, including restriction or removal of access to the platform, termination of contracts, or referral to relevant authorities where appropriate

Breaches of this Code may also be treated as safeguarding concerns

Review

This Code of Conduct is reviewed periodically and updated as required to reflect best practice and changes in guidance or legislation.

---

6. Serious Incident Reporting Policy

Purpose

To provide a clear framework for recognising and reporting serious incidents that may affect Allegr Ltd's reputation, operations, or legal compliance.

Scope

Applies to all directors and anyone representing Allegr Ltd in a professional capacity.

Definition of Serious Incident

Includes but is not limited to: data breaches, criminal allegations, serious injury, financial fraud, and any event likely to result in regulatory or reputational damage.

Procedure

1. Any serious incident must be reported to the Board immediately.
2. A Director will lead an initial review to determine the severity and next steps.
3. If needed, external advice (legal, regulatory) will be sought.
4. A record of the incident and response will be created and stored securely.
5. Learnings and preventative measures will be shared with the Board.

---

7. Privacy Policy

Allegr Ltd’s Privacy Policy can be found on our website:

https://www.militaryapp.org/policies/privacy-policy

Allegr’s Privacy Policy should seek to cover the following sections:

1. Information We Collect (Log Data, Device Data, Personal Information, User-Generated Content)
2. Legitimate Reasons for Processing Your Personal Information
3. Collection and Use of Information
4. Security of Your Personal Information
5. How Long We Keep Your Personal Information
6. Disclosure of Personal Information to Third Parties
7. Your Rights and Controlling Your Personal Information
8. Use of Cookies
9. Limits of Our Policy
10. Additional disclosures for General Data Protection Regulation (GDPR) compliance (EU)
11. Additional disclosures for Australian Privacy Act compliance (AU)
12. Additional disclosures for UK General Data Protection Regulation (UK GDPR) compliance (UK)
13. Data subject rights
14. Enquiries, reports and escalation

The Privacy Policy must be reviewed annually.

8. Software Development Security Policy

Purpose

This policy outlines our approach to integrating security at every stage of our software development process. It is based on the UK Government and MOD’s Secure by Design (SbD) principles and adapted to suit our small, agile team.

Our aim is to ensure security is embedded from the outset, not treated as a final checklist or compliance hurdle. This policy provides clear principles and actionable steps to support a consistent, risk-aware approach to secure development.

Our Security Principles

We adopt the following principles across our development and delivery lifecycle:

• Security is proactive: It starts at the idea stage and continues through the lifecycle of the product or feature.
• **Everyone is responsible:** Security is a shared responsibility across product, engineering, and operations - not siloed to one individual or team.

- **Proportionate, not perfect:** Security controls are scaled to the criticality and complexity of the system or feature being developed.
- **Assurance is continuous:** Risk is not “signed off” at go-live. We build, test, monitor, and adapt as systems evolve.
- **User safety matters:** We design systems that protect end-users - including their data, privacy, and interactions with others.

Checklist System Overview

To ensure our Secure by Design practices are applied consistently, we use a set of internal checklists to guide and document security considerations at key points in our development process. These checklists are accessed via our website (private) and completed as online forms.

Each submission is:

- Automatically converted to a PDF record
- Stored in our internal archive for audit purposes
- Attributed to the person submitting the form, with a timestamp

This approach provides traceability, accountability, and ongoing visibility into our secure development practices.

The three core checklists are described below and accessed here:
https://www.militaryapp.org/policies/software-checklist

1. New Feature Design Checklist

This checklist is completed before development begins on any new feature.
It ensures the team considers:

- What data the feature will handle
- Potential risks from misuse or breach
- Whether new APIs or external access points are introduced
- Whether any new roles or permissions are needed
- Whether the feature allows user-generated content or interaction
- Whether least-privilege access has been applied in both code and infrastructure

2. Release Readiness Checklist

Completed before deploying a feature to staging, beta, or production environments.
This checklist covers:

- Securing all communications (internal and external) with HTTPS/SSL
- Removal of hardcoded secrets or test credentials
- Input validation and sanitisation to prevent common attacks
- Enforcement of permissions on the server side (not just UI)
- Logging of key events for audit and monitoring

- Sensible default permissions for new users or roles
- T&Cs or consent requirements (if user-facing)
- A basic peer or automated security review

3. Quarterly Security Review Checklist
Conducted every three months as part of our continuous assurance process.
It includes:

- Reviewing and updating user permissions and admin roles
- Auditing use of third-party services, APIs, or integrations
- Reviewing data storage and encryption standards
- Assessing the adequacy of moderation tools and abuse handling
- Verifying our incident response plan and escalation process
- Ensuring T&Cs, privacy notices, and consent flows remain accurate
- Reviewing the effectiveness of our SbD checklists and refining them as needed

Review and Updates

This policy will be reviewed and updated on a biannual basis or after any significant change to our development processes, threat landscape, or MOD/security requirements.

---

9. Remuneration Policy

Purpose

This policy sets out Allegr Ltd’s approach to remuneration, ensuring it is fair, transparent, proportionate, and aligned with our purpose as a social enterprise operating in the charity and community sector.

Scope

This policy applies to:

- Directors of Allegr Ltd
- Any future employees or contractors, should they be engaged

Policy Statement

Allegr Ltd is a small social enterprise operating with limited resources and careful cash-flow management. We are committed to ensuring that remuneration:

- Is affordable and sustainable
- Reflects the responsibilities and time commitment of roles
- Supports the long-term viability of the organisation

- Does not compromise delivery of our social purpose

Director remuneration is kept under regular review and set at a level that is modest, justified, and appropriate to the size and financial position of the organisation.

Director Remuneration

- Allegr Ltd currently has three directors, two of whom receive remuneration for operational and executive responsibilities.
- Remuneration levels are agreed by the Board.
- Payments are made only where affordable and in line with current cash flow.
- Where sufficient cash is not available to meet director payroll, amounts may be credited to a Directors' Loan Account and paid when the financial position allows.
- No director receives performance-related bonuses or incentives linked to profit.

Expenses

Directors may claim reasonable, pre-approved expenses incurred wholly and exclusively in the course of Allegr Ltd business. All expense claims must be supported by appropriate records.

Financial Oversight and Transparency

- Remuneration decisions are made collectively by the Board and recorded in Board meeting minutes.
- The financial impact of remuneration is considered alongside operational needs and reserves.
- Director remuneration and loans are accounted for in line with legal and accounting requirements and disclosed where required.

Review

This policy is reviewed annually by the Board, or sooner if:

- There is a material change to the financial position of the organisation
- Employees are recruited
- Regulatory or governance expectations change

10. Reserves Policy

Purpose

The purpose of this policy is to explain Allegr Ltd's approach to holding and managing reserves, ensuring financial resilience, responsible governance, and the continued delivery of our services while operating within a constrained and variable cash-flow environment.

Scope

This policy applies to all unrestricted reserves of Allegr Ltd and is approved and overseen by the Board.

Policy Statement

Allegr Ltd is a small and growing social enterprise operating a digital community platform. We experience variable income and carefully manage cash flow while prioritising service delivery and platform development.

The Board recognises the importance of maintaining adequate reserves to manage risk and ensure continuity of operations. However, given our size, growth stage, and operating model, we do not currently maintain high levels of cash reserves. This position is actively managed and reviewed by the Board.

Definition of Reserves

Reserves are defined as unrestricted funds that are available to support the ongoing operations of Allegr Ltd.

In assessing reserves, the Board considers the totality of unrestricted resources, which may include:

- Cash at bank
- Accounts receivable, where collection is reasonably assured
- Other unrestricted assets recognised on the balance sheet, including the digital platform and associated intellectual property

Restricted funds and assets held for specific purposes are excluded from reserves.

Reserves Level and Rationale

The Board does not set a fixed cash-only reserves target. Instead, it assesses reserve adequacy by reference to:

- Forecast income and expenditure
- Cash-flow projections
- The timing and reliability of accounts receivable
- The nature, value, and strategic importance of non-cash assets
- Known and emerging financial risks

Given the organisation’s growth phase and income profile, the Board accepts that cash reserves may fall below levels typically recommended for more established organisations. This position is mitigated through:

- Active cash-flow management
- Regular financial monitoring
- The availability of Directors’ Loan Accounts where required
- Ongoing oversight of financial risk

The Board considers this approach to be reasonable, proportionate, and in the best interests of the organisation at its current stage of development.

Use of Reserves

Reserves may be used only for purposes consistent with Allegr Ltd’s objects and may include:

- Meeting short-term operational commitments
- Managing periods of delayed or uneven income
- Maintaining core services during financial uncertainty
- Strategic investment in platform development and infrastructure

Any significant use of reserves is approved by the Board and recorded in board minutes.

Monitoring and Governance

- The Board reviews reserve levels and cash-flow forecasts regularly as part of its financial oversight.
- Reserve levels are considered alongside the organisation’s risk register.
- The adequacy of reserves is explicitly reviewed at least annually and reported as part of governance and financial reporting.

Review

This policy is reviewed annually by the Board and updated as necessary to reflect:

- Changes in financial position or risk profile
- Growth in scale or complexity of operations
- Regulatory or best-practice guidance

11. EDI (Equality, Diversity & Inclusion) Policy

Purpose

The purpose of this policy is to promote equality, diversity, and inclusion in all areas of our work. We are committed to creating a fair, respectful, and inclusive environment for everyone who engages with our digital community platform and services.

Scope

This policy applies to all directors, employees, contractors, partners, users, and members of the public who interact with our services, platform, or business activities.

Policy Statement

We are committed to equality of opportunity and to preventing discrimination, harassment, or unfair treatment on the basis of protected characteristics as defined by the Equality Act 2010, including but not limited to age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, pregnancy or maternity, and marriage or civil partnership.

We value diversity and aim to foster an inclusive digital community where individuals are treated with dignity and respect. We expect all those engaging with our platform to uphold these principles.

Procedure

We take reasonable steps to ensure our services and platform are accessible and inclusive. Discriminatory behaviour, harassment, or exclusionary conduct will not be tolerated and may result in action in line with our terms of use or internal procedures.

Concerns or complaints relating to equality or inclusion can be raised through our complaints process or via the platform’s reporting tools.

This policy is reviewed periodically to ensure it remains appropriate and effective.

End of Policy Pack