BE(YOU)FULL CIC

Safeguarding Governance and Operational Policy Suite

England | Executive governance edition | October 2026

A modular, non-duplicative safeguarding framework for BE(YOU)FULL CIC. It is designed for organisational governance, programme delivery, partnerships, mentoring, education, research and digital activity involving children, young people and adults at risk.

Jurisdiction and legal position

This suite is written for BE(YOU)FULL CIC operations in England. It reflects current legislation and statutory guidance as at 2 October 2026. Where BE(YOU)FULL works in a school, college, local authority, NHS body or other regulated setting, the host organisation may have additional statutory or contractual requirements that take precedence where they impose a higher safeguarding standard.

The suite does not represent legal advice. Before formal adoption, the Board should confirm named safeguarding roles, reporting channels, insurance requirements, DBS eligibility for each role, local authority escalation routes and any commissioner-specific terms.

Suite architecture

- 01 Core Safeguarding and Participant Safety Policy - principles, scope, governance and legal framework.
- 02 Safeguarding Reporting, Escalation and Case Management Procedure - what happens when a concern arises, including adults at risk, allegations, low-level concerns and information sharing.
- 03 Code of Conduct and Professional Boundaries - behavioural expectations for directors, staff, associates, mentors, coaches and volunteers.
- 04 Safer Recruitment, Vetting and DBS Policy - role risk assessment, recruitment controls, DBS checks and referral duties.
- 05 Digital Safeguarding, Online Delivery and Media Standard - online sessions, digital communications, photography, video and consent.
- 06 Whistleblowing and Speaking Up Policy - confidential escalation of wrongdoing or unsafe practice.
- 07 Partner and Contractor Safeguarding Standard - minimum requirements for delivery partners, suppliers and associates.
- 08 Safeguarding Concern and Incident Record - operational recording template.

01

Core Safeguarding and Participant Safety Policy

The governing policy for all BE(YOU)FULL safeguarding activity. Supporting documents implement this policy and do not repeat it.

Document owner	Safeguarding Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Purpose

BE(YOU)FULL CIC is committed to protecting children, young people, adults at risk and other participants from abuse, neglect, exploitation, harassment, discrimination and avoidable harm. Safeguarding is a governance responsibility, an operational discipline and a condition of ethical delivery. It applies to how BE(YOU)FULL designs programmes, selects people, manages partnerships, communicates online, handles information, responds to concerns and learns from incidents.

2. Scope

This policy applies to all directors, employees, workers, consultants, contractors, mentors, coaches, researchers, facilitators, volunteers, students on placement and delivery partners acting for or on behalf of BE(YOU)FULL CIC. It applies to in-person, online, hybrid, outreach, research, mentoring, training, community and partnership activity.

3. Safeguarding principles

- Safeguarding is everyone’s responsibility. Concerns are acted on promptly and are not treated as matters to be resolved informally where a person may be at risk.
- Practice is person-centred and, for children, child-centred. The welfare and best interests of the person at risk take priority over organisational reputation, convenience or commercial interest.
- BE(YOU)FULL uses the least intrusive response consistent with safety, legal duties and professional standards, while recognising that consent is not required to share information where there is a lawful safeguarding necessity.
- Discrimination, racism, harassment, sexual misconduct, bullying, exploitation and abuse of power are safeguarding concerns where they create or compound risk of harm.
- Participants are treated with dignity and are informed, in accessible language, how to raise concerns and what will happen next.

- No person will be disadvantaged for raising a safeguarding concern in good faith.

4. Definitions

Child: a person under 18. Adult at risk: for the purposes of this suite, an adult who has needs for care and support, is experiencing or at risk of abuse or neglect, and because of those needs may be unable to protect themselves; this reflects the safeguarding framework in the Care Act 2014. Safeguarding concern: information suggesting that a person has been harmed, may be harmed, may be at risk of abuse or neglect, or that a worker's conduct may be unsafe or incompatible with their role. Regulated activity: activity falling within the statutory definitions for children or adults under the Safeguarding Vulnerable Groups Act 2006, as amended.

5. Governance and accountability

- The Board retains ultimate accountability for safeguarding governance and must receive at least an annual safeguarding assurance report.
- A Designated Safeguarding Lead (DSL) must be formally appointed before BE(YOU)FULL undertakes delivery involving children or adults at risk. A deputy or alternative escalation route must be defined so that no concern depends on one individual being available.
- The DSL owns operational safeguarding practice, triage, referral quality, case oversight, training standards and safeguarding records. The DSL does not investigate suspected crimes or substitute for children's social care, adult safeguarding services, police or statutory agencies.
- Programme leads are accountable for programme-level risk assessments, participant information, consent processes, safe staffing and compliance with this suite.
- All safeguarding incidents, near misses, allegations and material concerns must be captured in the safeguarding record system and reviewed for organisational learning.

6. Legal and statutory framework

The suite is informed by, and where legally applicable gives effect to, the following framework. The precise duty applying to BE(YOU)FULL depends on the activity, commissioning arrangement and setting:

- Children Act 1989 and Children Act 2004 - the wider legal framework for safeguarding and promoting children's welfare in England.
- Working Together to Safeguard Children 2026 - statutory guidance on multi-agency help, support and protection for children; BE(YOU)FULL will work consistently with its expectations when engaging with safeguarding partners and relevant agencies.
- Keeping Children Safe in Education 2026 - statutory guidance for schools and colleges. BE(YOU)FULL is not automatically subject to every KCSIE duty as a CIC, but will meet host-setting requirements and apply KCSIE-aligned standards when delivering in or for schools and colleges.
- Safeguarding Vulnerable Groups Act 2006, as amended by the Protection of Freedoms Act 2012 - regulated activity, barred-list safeguards and referral duties.
- Care Act 2014, including section 42 - the statutory safeguarding framework for adults at risk in England; local authorities hold the section 42 enquiry duty.
- Data Protection Act 2018 and UK GDPR - lawful, fair and secure processing of personal and special-category data, including safeguarding information.
- Department for Education statutory information-sharing guidance in force from September 2026 - safeguarding information should be shared lawfully, proportionately and without inappropriate delay.
- Equality Act 2010 and Human Rights Act 1998 - non-discrimination, dignity and proportionate decision-making.
- Employment Rights Act 1996 as amended by the Public Interest Disclosure Act 1998 - statutory protection for qualifying whistleblowing disclosures.
- Counter-Terrorism and Security Act 2015 and current Prevent duty guidance - directly applicable only where BE(YOU)FULL is itself within scope as a specified authority; otherwise relevant where BE(YOU)FULL

delivers under the safeguarding arrangements of a specified authority or where contractual requirements apply.

7. Risk management and programme design

- Every programme involving children or adults at risk must have a proportionate safeguarding risk assessment before delivery begins.
- Risk assessment must consider location, one-to-one contact, transport, online contact, photography, access needs, protected characteristics, power imbalances, staff ratios, lone working, data handling and escalation routes.
- Where delivery takes place in a host institution, responsibilities for safeguarding, referrals, emergency response, attendance information, parental/carer communication and allegations management must be agreed before delivery.
- High-risk delivery must not begin until the DSL is satisfied that controls are adequate.

8. Reporting and response

All concerns must be handled under Document 02. Immediate danger or suspected serious crime requires emergency or police action where appropriate. Staff must not promise confidentiality, conduct their own investigation, confront an alleged perpetrator, or delay a referral in order to secure complete information.

9. Recruitment, conduct and digital practice

Recruitment and vetting are governed by Document 04. Behavioural expectations and professional boundaries are governed by Document 03. Online delivery, digital communications, photography and media are governed by Document 05.

10. Information governance

- Safeguarding records must be factual, timely, access-controlled and stored separately from routine programme notes where practicable.
- Only information necessary for safeguarding, legal compliance, referral or case management should be shared, and only with those who need it.
- Consent should be sought where appropriate, but lack of consent must not prevent lawful sharing where there is a safeguarding necessity, legal obligation, vital-interest concern or other applicable lawful basis.
- Record retention must follow the organisation’s retention schedule and any commissioner, insurer or statutory requirement.

11. Training and assurance

- All personnel must receive safeguarding induction appropriate to their role before unsupervised contact with participants.
- Personnel working with children must understand indicators of abuse, neglect, exploitation, child-on-child abuse, sexual harassment, online harm and the requirement to report concerns immediately.
- Role-specific refresher training must be scheduled according to risk and commissioner requirements, with annual confirmation that procedures remain understood.
- The Board will review safeguarding assurance at least annually and after any serious incident, significant complaint, regulatory change or material delivery change.

02

Safeguarding Reporting, Escalation and Case Management Procedure

One operational procedure covering child safeguarding, adult safeguarding, allegations, low-level concerns, information sharing and case closure.

Document owner	Safeguarding Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Immediate response

1. If anyone is in immediate danger, call 999 or take proportionate emergency action without waiting for internal authorisation.
2. Listen calmly. Do not investigate, interrogate, ask leading questions or promise secrecy.
3. Record the person's own words as accurately as possible, distinguishing fact, observation and opinion.
4. Report to the DSL immediately, or to the deputy/Board safeguarding contact if the concern involves the DSL or the DSL is unavailable.

2. DSL triage

The DSL will assess urgency, immediate protective measures, the need for statutory referral, police involvement, host-setting notification, parent/carer communication where appropriate, DBS implications, contractual notification and information-sharing requirements. The DSL records the rationale for the decision, including decisions not to refer.

3. Concerns about a child

Where there is reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm, the matter must be referred promptly through the appropriate local safeguarding route. BE(YOU)FULL will not delay referral while attempting to establish proof. Where the activity is delivered in a school or college, the host DSL must normally be informed in accordance with the agreed safeguarding protocol, without displacing BE(YOU)FULL's responsibility to act if urgent action is required.

4. Concerns about an adult at risk

Where the concern meets or may meet the Care Act safeguarding threshold, the DSL should contact the relevant local authority adult safeguarding service and/or emergency services as appropriate. The adult's wishes should be taken seriously, but safety, coercion, capacity, risk to others, public interest and legal duties may justify action without consent.

5. Allegations against staff, volunteers, contractors or associates

- An allegation that a person working for BE(YOU)FULL has harmed a child or adult at risk, may pose a risk of harm, may have committed an offence against or related to a child or adult at risk, or behaved in a way indicating unsuitability must be escalated immediately.
- The person who is the subject of the allegation must not lead or influence the safeguarding response.
- Where the allegation relates to a child and meets the relevant threshold, the DSL/authorised senior officer will liaise with the local authority designated officer or equivalent local authority allegations function as appropriate to the setting and local arrangements.
- Employment or contractual action must be coordinated with safeguarding and statutory processes so that internal action does not compromise evidence or statutory enquiries.
- Where the statutory DBS referral conditions are met, BE(YOU)FULL must make a barring referral even if another body has also been notified.

6. Low-level concerns

A low-level concern is behaviour that is inconsistent with the Code of Conduct or expected professional boundaries but may not meet the threshold for a formal allegation. Low-level concerns must still be recorded and reviewed. Patterns, repeated boundary breaches, grooming-type behaviour, retaliation or escalation must be reconsidered as potential safeguarding allegations. The label "low-level" describes the apparent threshold, not the importance of recording and reviewing the concern.

7. Information sharing

- Share information on a need-to-know basis, using the minimum information necessary to achieve the safeguarding purpose.
- Do not use data protection as a reason to withhold information where lawful sharing is necessary to protect a child or adult at risk.
- Record what was shared, with whom, when, the lawful rationale and any restrictions on onward disclosure.
- Where consent is not obtained, record why sharing without consent was necessary and proportionate.

8. Case management and closure

Each case must have a unique reference, chronology, decisions, referrals, actions, outcomes and closure rationale. Closure occurs only when immediate risk is managed, required referrals have been completed, employment/contractual actions are tracked, participant support needs are considered, and any organisational learning has been assigned. Serious incidents and recurring patterns must be reported to the Board in an appropriately anonymised form unless identifiable information is necessary for governance action.

03

Code of Conduct and Professional Boundaries

Mandatory behavioural standard for everyone acting for BE(YOU)FULL CIC.

Document owner	Safeguarding Lead / People Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Required conduct

- Treat every participant with dignity, respect, fairness and professional care.
- Maintain clear role boundaries and avoid creating dependency, exclusivity or secrecy.
- Use language, touch, humour and communication that are appropriate to the participant, context and professional purpose.
- Challenge discriminatory, degrading, sexualised, bullying or abusive behaviour.
- Use only approved communication channels and follow the Digital Safeguarding Standard.
- Report safeguarding concerns, boundary breaches and unsafe practice immediately.

2. Prohibited conduct

- Entering into sexual or romantic relationships with children, or exploiting any participant through a professional power imbalance.
- Sexualised comments, grooming behaviour, harassment, coercion, threats, intimidation, humiliation or discriminatory abuse.
- Giving personal contact details to children or using private social-media messaging outside approved arrangements.
- Unapproved one-to-one meetings in isolated locations, transporting participants without authorisation, or inviting participants to a private home.
- Photographing, filming or recording participants on personal devices unless expressly authorised under the Media Standard.
- Providing alcohol, illegal drugs, age-restricted products or inappropriate gifts to participants.
- Accepting gifts, money or favours that could compromise professional judgement or create an obligation.
- Investigating a disclosure or asking a participant to repeat traumatic details unnecessarily.
- Retaliating against any person who raises a concern.

3. One-to-one mentoring and coaching

One-to-one work must have a defined purpose, agreed boundaries, documented scheduling and a safe setting. For children, arrangements must follow the programme risk assessment and host/parental requirements. Unscheduled private contact, hidden communications and meetings outside approved arrangements are not permitted.

4. Breaches

A breach may result in safeguarding action, suspension from delivery, disciplinary or contractual action, referral to a host organisation, local authority, police, professional regulator or DBS, and termination of engagement. The response will be proportionate to risk and legal duties.

04

Safer Recruitment, Vetting and DBS Policy

Risk-led recruitment controls for employees, workers, volunteers, associates and contractors.

Document owner	People Lead / Safeguarding Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Recruitment principle

No appointment decision will be based on a DBS certificate alone. Safer recruitment combines role design, identity verification, employment/experience history, references, interview assessment, conflict-of-interest checks, qualification checks where relevant, safeguarding questions and the legally appropriate level of DBS check.

2. Role risk assessment

- Every role must be assessed before recruitment to determine participant contact, level of supervision, frequency, location, access to sensitive information, regulated-activity status and DBS eligibility.
- BE(YOU)FULL will request only the level of criminal-record check for which the role is legally eligible.
- Where barred-list information is required for regulated activity, the organisation will ensure the role meets the statutory criteria before requesting it.

3. Minimum recruitment controls

- Written role description and safeguarding responsibilities.
- Identity and right-to-work verification where applicable.
- At least two references for roles with significant participant contact where practicable, including a recent professional reference.
- Exploration of unexplained gaps or inconsistencies in work/volunteering history.
- Qualification and professional registration checks where relevant.
- Safeguarding suitability questions at interview for roles involving children or adults at risk.
- DBS or other criminal-record check at the correct level where legally eligible and proportionate.
- Signed Code of Conduct and confidentiality/data-protection obligations before delivery.

4. DBS information and decisions

Disclosure information is sensitive personal data. Access must be restricted to those who need it for the recruitment decision. A criminal record does not automatically bar appointment unless the law prohibits the person from the relevant work. Decisions must be risk-based, relevant to the role, proportionate and documented.

5. Barred persons and referral duty

BE(YOU)FULL must never knowingly permit a barred person to engage in regulated activity from which they are barred. Where BE(YOU)FULL is a regulated activity provider and the statutory referral conditions are met - including removal from regulated activity (or where removal would have occurred had the person not left) together with relevant conduct, the harm test or a relevant offence - a DBS referral is a legal duty and must not be displaced by a referral to another body.

6. Ongoing suitability

Safeguarding suitability continues after recruitment. Personnel must disclose matters that may affect their suitability where lawfully required by the role or contractual terms. Changes in duties must trigger reconsideration of DBS eligibility and safeguarding risk. Re-checking arrangements will follow legal eligibility, commissioner requirements and assessed risk rather than an arbitrary universal interval.

05

Digital Safeguarding, Online Delivery and Media Standard

Rules for online sessions, messaging, platforms, photography, video, audio and public communications.

Document owner	Safeguarding Lead / Digital Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Approved digital environments

- Use organisation-approved accounts, platforms and devices where practicable.
- For work with children, avoid private one-to-one messaging through personal social-media accounts or disappearing-message functions.
- Online sessions must have clear attendance, identity, moderation and escalation arrangements proportionate to risk.
- Where sessions are recorded, participants must be told in advance why, how the recording will be used, who can access it and how long it will be retained.

2. Online professional boundaries

The same professional standards apply online as in person. Staff must not develop informal private relationships with participants, move conversations to personal channels, share inappropriate content, or communicate at unreasonable times except for a documented operational necessity.

3. Images, video and audio

- Capture only where there is a defined purpose and an appropriate lawful basis and consent/permission process where required.
- For children, follow the programme's parental/carer permission and child-assent arrangements unless another lawful basis is specifically established.
- Do not publish identifying safeguarding information, sensitive case details or images that create avoidable risk.
- Personal devices must not be used for participant imagery unless expressly authorised and subject to immediate secure transfer and deletion controls.
- Withdrawal of consent must be respected for future use where consent is the lawful basis, subject to material already lawfully published or other legal constraints.

4. Online harm and disclosures

Concerns about grooming, sexual exploitation, coercion, threats, self-generated sexual imagery involving children, cyberbullying, stalking, doxxing, extremist content or other online harm must be escalated through Document 02. Staff should preserve relevant evidence where safe and lawful but must not circulate harmful content unnecessarily.

06

Whistleblowing and Speaking Up Policy

Confidential route for concerns about wrongdoing, safeguarding failures, cover-up or unsafe organisational practice.

Document owner	Board / People Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Purpose

BE(YOU)FULL encourages personnel to speak up where they reasonably believe there is wrongdoing, danger, safeguarding failure, unlawful conduct, financial impropriety, serious data misuse, concealment or retaliation. Safeguarding concerns about an individual participant or worker should also be reported under Document 02; whistleblowing is an additional route where the concern relates to organisational practice, leadership, cover-up or inability to use normal channels safely.

2. Routes

- Raise the concern with the line manager or programme lead where appropriate.
- Raise directly with the DSL where safeguarding is involved.
- Raise with the Board safeguarding contact/Chair-equivalent where the concern involves senior management or the DSL.
- Use an appropriate external prescribed person, regulator, statutory agency or emergency service where legally protected or necessary; staff are not required to remain silent where external reporting is lawful and justified.

3. Protection and confidentiality

No person will be subjected to retaliation for raising a concern in good faith. Confidentiality will be protected as far as reasonably possible, but absolute anonymity cannot be guaranteed where disclosure is necessary for a fair process, statutory referral or protection from harm. Deliberately malicious allegations may be addressed through conduct procedures; an unsubstantiated concern raised honestly is not misconduct.

07

Partner and Contractor Safeguarding Standard

Minimum safeguarding controls for organisations and individuals delivering with or on behalf of BE(YOU)FULL CIC.

Document owner	Safeguarding Lead / Partnerships Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

1. Applicability

This standard applies where a partner, subcontractor, venue provider, freelancer or associate has participant contact, access to safeguarding information, or responsibility for activity involving children or adults at risk.

2. Minimum requirements

- Named safeguarding lead and escalation route appropriate to the partner's size and role.
- Current safeguarding policy and procedures appropriate to the participant group and activity.
- Safer recruitment and lawful DBS arrangements for relevant personnel.
- Code of conduct and professional-boundary expectations at least equivalent to BE(YOU)FULL's standard.
- Immediate notification to BE(YOU)FULL of safeguarding incidents connected to joint delivery, subject to lawful information sharing.
- Cooperation with statutory referrals, allegations management, serious-incident review and commissioner requirements.
- Compliance with data-protection obligations and secure handling of safeguarding records.
- No subcontracting of participant-facing safeguarding responsibilities without prior approval where the contract requires it.

3. Due diligence and contracting

Safeguarding due diligence must be proportionate to risk and completed before delivery. Contracts or partnership agreements must allocate safeguarding responsibilities, reporting deadlines, data-sharing expectations, DBS responsibilities, insurance where relevant, audit rights and termination/suspension rights for safeguarding breach.

08

Safeguarding Concern and Incident Record

Controlled template for recording concerns, disclosures, allegations, decisions and referrals. Store securely; do not publish completed forms.

Document owner	Safeguarding Lead
Approval authority	Board of Directors
Version	1.0
Approved	October 2026
Next review	October 2027, or earlier following material legal, regulatory or operational change
Status	Board-ready draft for formal approval

Case reference	
Date/time concern received	
Person completing record	
Programme / location / online platform	
Person(s) at risk	
Age / date of birth if known	
Parent/carer details if relevant	
Nature of concern	
Immediate safety action taken	
What was seen/heard/disclosed (factual account; use the person's own words where possible)	
Other witnesses / sources	
DSL notified - date/time	
Decision and rationale	
External referral(s) - agency / date / reference	

Host organisation notified - if applicable	
Parent/carer communication - if applicable and safe	
Police / emergency services involvement	
DBS referral consideration / outcome	
Support offered to participant	
Employment / contractor action, if any	
Information shared - what / with whom / lawful rationale	
Follow-up actions / owner / deadline	
Case closure date and rationale	
Learning / control improvements	

Legal and guidance references

- Children Act 1989.
- Children Act 2004.
- Working Together to Safeguard Children 2026, Department for Education (England).
- Keeping Children Safe in Education 2026, Department for Education (England) - applicable directly to schools and colleges and used by BE(YOU)FULL as an aligned standard when delivering in those settings.
- Safeguarding Vulnerable Groups Act 2006, as amended, including regulated activity and barring provisions.
- Protection of Freedoms Act 2012.
- Care Act 2014, including section 42 safeguarding enquiries.
- Data Protection Act 2018 and UK GDPR.
- Department for Education statutory guidance on information sharing to safeguard children and young people, in force from September 2026.
- Equality Act 2010.
- Human Rights Act 1998.
- Employment Rights Act 1996 and Public Interest Disclosure Act 1998.
- Counter-Terrorism and Security Act 2015 and Prevent duty guidance for England and Wales (2023), where applicable.
- Disclosure and Barring Service guidance on regulated activity and legal referral duties, updated September 2026.

Governance note: statutory guidance and role eligibility can change. The DSL and Board should verify current GOV.UK/legislation.gov.uk requirements at each annual review and before materially changing participant-facing delivery.