



DEPARTMENT	OPERATIONS
POLICY/PROCEDURE	SAFEGUARDING POLICY (INCLUDING ARTIFICIAL INTELLIGENCE & SOCIAL MEDIA)
DATE OF ISSUE	AUGUST 2026
DATE OF REVIEW	AUGUST 2028
VERSION	1

1. Policy Statement

Lincoln City Football Club is committed to providing a safe, supportive, and inclusive environment for all children, young people, and vulnerable adults with whom we work. We recognise our responsibility to protect individuals from abuse, neglect, exploitation, harm, and inappropriate conduct whether these occur in person, online, through social media platforms, or via Artificial Intelligence (AI) technologies.

Safeguarding is everyone's responsibility. All staff, volunteers, contractors, trustees, and third parties acting on behalf of the organisation must promote the welfare of those in our care and take appropriate action where concerns arise.

2. Purpose

This policy aims to:

- Protect children, young people, and vulnerable adults from harm.
- Ensure staff understand their safeguarding responsibilities.
- Promote safe use of technology, social media, and AI systems.
- Establish clear procedures for reporting safeguarding concerns.
- Ensure compliance with relevant legislation and best practice guidance.
- Maintain a culture where safeguarding is embedded in all activities.

3. Scope

This policy applies to:

- Employees
- Volunteers
- Trustees and directors
- Students and work experience placements
- Service users
- Anyone acting on behalf of the organisation

The policy applies to all activities, including:

- Face-to-face interactions
- Remote and online services
- Social media use
- AI-enabled systems and applications
- Digital communications

4. Definitions

Safeguarding

Safeguarding means protecting an individual's right to live free from abuse, harm, neglect, exploitation, bullying, discrimination, and inappropriate treatment.

Child

Anyone under the age of 18.

Vulnerable Adult

An individual aged 18 or over who may need support due to age, illness, disability, mental health needs, or other circumstances.

Artificial Intelligence (AI)

Technology capable of generating, analysing, processing, or assisting with content, decisions, communications, or tasks using machine-learning or automated systems.

Social Media



DEPARTMENT	OPERATIONS
POLICY/PROCEDURE	SAFEGUARDING POLICY (INCLUDING ARTIFICIAL INTELLIGENCE & SOCIAL MEDIA)
DATE OF ISSUE	AUGUST 2026
DATE OF REVIEW	AUGUST 2028
VERSION	1

Any digital platform used for communication, networking, content sharing, messaging, or public engagement, including but not limited to Facebook, Instagram, TikTok, X, LinkedIn, Snapchat, YouTube, WhatsApp, and similar services.

5. Safeguarding Principles

The organisation will:

- Put the welfare of individuals first.
- Listen to and take concerns seriously.
- Act promptly on safeguarding issues.
- Work in partnership with parents, carers, agencies, and authorities where appropriate.
- Promote a culture of respect, dignity, and inclusion.
- Ensure safeguarding considerations are incorporated into all digital activities.

6. Roles and Responsibilities

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Managing safeguarding concerns and referrals.
- Maintaining safeguarding records.
- Providing advice and support to staff.
- Liaising with statutory agencies.

Club

Club must:

- Promote safeguarding awareness.
- Respond appropriately to safeguarding concerns.

Staff and Volunteers

All staff and volunteers must:

- Report concerns immediately.
- Maintain professional boundaries.
- Use social media and AI responsibly.
- Follow organisational procedures.

7. Recognising Safeguarding Concerns

Concerns may include:

- Physical abuse
- Emotional abuse
- Sexual abuse
- Neglect
- Financial exploitation
- Domestic abuse
- Radicalisation
- Bullying or cyberbullying



DEPARTMENT	OPERATIONS
POLICY/PROCEDURE	SAFEGUARDING POLICY (INCLUDING ARTIFICIAL INTELLIGENCE & SOCIAL MEDIA)
DATE OF ISSUE	AUGUST 2026
DATE OF REVIEW	AUGUST 2028
VERSION	1

- Online grooming
- Sextortion
- Harassment
- Discriminatory behaviour
- AI-enabled exploitation or manipulation

Any concerns should be reported immediately to the DSL.

8. Online Safety and Digital Safeguarding

The organisation recognises that safeguarding risks increasingly occur online.

Potential risks include:

- Cyberbullying
- Grooming
- Online exploitation
- Exposure to harmful content
- Identity theft
- Fraud and scams
- Misuse of personal data
- Unauthorised sharing of images or information

The organisation will:

- Promote safe digital practices.
- Use secure systems where possible.
- Limit access to sensitive information.
- Educate staff and service users about online risks.
- Investigate digital safeguarding concerns promptly.

9. Social Media Safeguarding

Professional Conduct

Staff and volunteers must:

- Maintain professional boundaries online.
- Avoid personal social media relationships with service users where inappropriate.
- Use approved organisational accounts when communicating on behalf of the organisation.
- Consider privacy and safeguarding implications before posting content.

Prohibited Activities

Staff must not:

- Share confidential or personal information.
- Publish images or information without appropriate consent.
- Harass, intimidate, or discriminate against others online.
- Engage in inappropriate discussions with children or vulnerable adults.



DEPARTMENT	OPERATIONS
POLICY/PROCEDURE	SAFEGUARDING POLICY (INCLUDING ARTIFICIAL INTELLIGENCE & SOCIAL MEDIA
DATE OF ISSUE	AUGUST 2026
DATE OF REVIEW	AUGUST 2028
VERSION	1

- Use personal accounts to communicate privately with service users unless expressly authorised.

Reporting

Any concerns involving:

- Cyberbullying
- Online abuse
- Threatening communications
- Inappropriate online contact
- Social media exploitation

must be reported immediately to the DSL.

10. Artificial Intelligence (AI) Safeguarding

Principles

The organisation recognises that AI can create opportunities but also safeguarding risks.

AI must be used in ways that:

- Protect individuals from harm.
- Preserve privacy and confidentiality.
- Respect human rights and dignity.
- Avoid discrimination and bias.
- Maintain appropriate human oversight.

Acceptable Use

AI tools may be used to:

- Assist with administration.
- Support communication drafting.
- Analyse non-sensitive information.
- Improve operational efficiency.

Human review must always be applied before decisions are acted upon.

Prohibited Use

Staff must not:

- Upload confidential or personal information into public AI tools without authorisation.
- Use AI to make safeguarding decisions without human oversight.
- Use AI-generated content to deceive, manipulate, or mislead.
- Create synthetic images, videos, or audio designed to exploit, harass, or impersonate individuals.
- Use AI to monitor individuals in a way that infringes legal or ethical standards.

AI Safeguarding Risks

Particular attention should be given to:

- Deepfakes
- AI-generated abuse material
- Identity impersonation
- Automated harassment



DEPARTMENT	OPERATIONS
POLICY/PROCEDURE	SAFEGUARDING POLICY (INCLUDING ARTIFICIAL INTELLIGENCE & SOCIAL MEDIA
DATE OF ISSUE	AUGUST 2026
DATE OF REVIEW	AUGUST 2028
VERSION	1

- Biased decision-making
- Inaccurate information (hallucinations)
- Disclosure of sensitive data

Any concerns relating to AI misuse must be reported immediately to the DSL.

11. Confidentiality and Data Protection

Safeguarding information will be:

- Shared only on a need-to-know basis.
- Stored securely.
- Processed in compliance with applicable data protection laws.
- Protected from unauthorised access.

Confidentiality should never prevent legitimate safeguarding concerns from being reported.

12. Reporting Procedure

Where a safeguarding concern arises:

1. Ensure any immediate danger is addressed.
2. Report the concern to the Designated Safeguarding Lead immediately.
3. Record factual information accurately.
4. Do not investigate independently unless authorised.
5. Maintain confidentiality.
6. Cooperate with any subsequent investigation.

If the concern relates to the DSL, it should be reported to a senior manager, or governing body representative.

13. Allegations Against Staff or Volunteers

Any allegation involving staff, volunteers, contractors, or trustees will be:

- Taken seriously.
- Assessed promptly.
- Managed confidentially.
- Referred to relevant authorities where required.
- Investigated in accordance with disciplinary procedures.

Where online conduct, social media activity, or AI misuse is involved, digital evidence should be preserved where possible.

14. Training

The organisation will provide:

- Safeguarding induction training.
- Specialist training for safeguarding leads.

15. Monitoring and Review

The organisation will:

- Review safeguarding incidents and trends.
- Monitor emerging digital, social media, and AI risks.



DEPARTMENT	OPERATIONS
POLICY/PROCEDURE	SAFEGUARDING POLICY (INCLUDING ARTIFICIAL INTELLIGENCE & SOCIAL MEDIA
DATE OF ISSUE	AUGUST 2026
DATE OF REVIEW	AUGUST 2028
VERSION	1

- Update this policy at least annually or sooner if required.
- Promote continuous improvement in safeguarding practices.

16. Related Policies

This policy should be read alongside:

- Code of Conduct Policy
- Data Protection Policy
- Safeguarding Children Policy
- Adults at Risk Policy
- Whistleblowing Policy
- Equality and Diversity Policy
- Safer Recruitment Policy

Next Review Date: ____August 2028__