SAFEGUARDING POLICY

Commitment to Safety

1. The Cyber Trust (the 'Organisation') works actively to prevent harm and promote the welfare of all children and adults at risk that we interact with (i.e. as The Cyber Trust's service users). This Safeguarding Policy applies to individuals referred to as 'Beneficiaries'.

2. The Organisation is committed to ensuring the safety and well-being of all the Beneficiaries, free from discrimination based on age, disability, race, religion, sexual orientation, gender identity, or any other protected characteristic.

3. This Safeguarding Policy adheres to the latest safeguarding laws of England, Wales, Northern Ireland, and Scotland, including relevant government guidance. If there is any conflict between this Policy and these laws, The Cyber Trust will always prioritise upholding the legal requirements.

4. The Cyber Trust has implemented this Safeguarding Policy in fulfilment of its obligations as a charity regulated by the Charity Commission for England and Wales (The Cyber Trust is registered with the Charity Commission with charity number 1171883).

5. For questions about this policy, please contact Dr Robert Nowill in the first instance, via e-mail info@thecybertrust.org or via phone 07477534532.

Safeguarding Policy Scope

6. This Policy applies to everyone working for or representing The Cyber Trust in the UK, regardless of position, employment type (full-time, part-time, temporary), or affiliation (direct employee, contractor, volunteer, intern; collectively 'Staff Members').

7. This Policy is separate from employment contracts. To ensure its effectiveness, The Cyber Trust may revise the Policy at any time. We will communicate any changes transparently.

8. This Policy outlines The Cyber Trust's approach to harm prevention for its Beneficiaries through Staff Member's conduct and practices.

9. This Safeguarding Policy applies to the organisation and operation of all The Cyber Trust activities that involve children and adults at risk (i.e. Relevant Activities). These primarily include:

a. Cyber safety education, training, research and games

Safeguarding Definition

10. The term 'Safeguarding' refers to practices and procedures designed to protect vulnerable individuals from harm or potential harm. It also promotes their overall well-being. Safeguarding is particularly crucial for children and adults at risk, with most legal obligations related to their care. This Policy specifically addresses:

a. Children, who are individuals under 18 years old (in England, Wales, and Northern Ireland) or under 16 years old (in Scotland).
b. Adults at risk, who are individuals 18 years old or over (in England, Wales, and Northern Ireland) or 16 years old or over (in Scotland) who require care and support, and due to this, are unable to protect themselves from harm (e.g. illness, disability). This can be temporary or permanent.

11. This Safeguarding Policy outlines The Cyber Trust's commitment to protecting its beneficiaries from harm caused by:

a. The Cyber Trust activities, practices, and the potential for harm arising from the conduct of its Staff Members, or
b. People and situations beyond (The Cyber Trust) and its Staff Members' control. This includes instances where Staff Members are aware of, ought to be aware of, or reasonably suspect a situation that poses a safeguarding risk.

12. This policy defines a 'Safeguarding Concern' as any conduct or situation that a Staff Member or someone else suspects might violate the safeguarding commitments above.

How The Cyber Trust Protects Its Beneficiaries: Key Safeguarding Measures

13. Prioritising child safety by following local safeguarding arrangements. These comprehensive plans, developed by local authorities, police, and healthcare providers, offer valuable leadership and guidance to ensure children's well-being.

14. Prioritising safeguarding adults by applying leadership and guidance provided by local Safeguarding Adults Boards.

15. All Staff Members will receive training on identifying and reporting safeguarding

concerns. Also, The Cyber Trust encourages them to report any Safeguarding Concerns they identify (set out below under the heading 'Procedures: Reporting').

16. We create a safe, accessible, fair, and efficient space for all Staff Members to raise safeguarding concerns (colleagues, beneficiaries, or anyone else involved). We expect all staff to listen attentively and professionally. Training will equip Staff Members to support those raising concerns and guide them through The Cyber Trust's established reporting procedures. All reported concerns will be handled by designated individuals and teams following The Cyber Trust's relevant procedures (detailed below under 'Procedures: Investigation and Response').

a. The Cyber Trust has fair and objective procedures to address all safeguarding concerns, even when they involve Staff Members. Allegations are taken seriously, with the severity of the claims considered throughout the process. We are committed to protecting all parties involved. This means we will only presume guilt or publicly criticise people once a thorough investigation is completed.

b. Reports that qualify as protected disclosures under whistleblowing law will be handled with the utmost confidentiality and following all relevant whistleblowing policies law.

17. Dr Robert Nowill is designated as the lead for safeguarding policies and procedures within The Cyber Trust.

18. Following appropriate recruitment processes for all new staff members, including volunteers. These processes include:

a. Conducting pre-employment checks following relevant regulations.

b. All new Staff Members must take part in, and understand the content of, all necessary safeguarding training before having any contact with The Cyber Trust's Beneficiaries. This training equips them with the knowledge and skills to keep everyone safe.

c. Following The Cyber Trust's staff recruitment and selection procedures.

19. Every Staff Member should be provided with, and required to undertake, training that is appropriate to their role, responsibilities, and degree and type of contact with Beneficiaries. This should, if appropriate, include training on:

a. Identify and respond to abuse by recognising signs of physical, emotional and sexual abuse, neglect, and exploitation.

b. Learn active listening skills and how to navigate disclosure of safeguarding concerns,

including confidentiality.

c. Follow reporting procedures by understanding when and how to report concerns using The Cyber Trust's established procedures.

d. Stay informed by discovering additional resources like policies, documents, and external training to stay up-to-date on safeguarding best practices.

20. Treating all safeguarding information with the utmost confidentiality and security. This involves:

a. Complying with UK data protection legislation, including The UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

b. Following The Cyber Trust's data protection policies and procedures.

c. Providing Staff Members with training on data protection and privacy, if appropriate.

d. Making easy to access Dr Robert Nowill, who can be contacted by emailing info@thecybertrust.org or at 07477534532 for Staff Members as an identifiable point of contact for questions or concerns about data protection and privacy.

e. Sharing safeguarding information internally ONLY on a strict need-to-know basis to ensure the best possible care for the beneficiary involved.

21. Building a safe environment by creating a culture of transparency and awareness to prevent harm. For example:

a. Encourage open communication by informing beneficiaries about The Cyber Trust's safeguarding procedures and how to report any concerns.

b. Acknowledge by the Staff Members of safeguarding laws, The Cyber Trust's safeguarding commitments and procedures, and Staff Members' responsibilities concerning these.

22. Regularly reviewing all safeguarding policies and procedures to ensure that they are up-to-date with safeguarding law and that they remain suitable for The Cyber Trust's Relevant Activities and workforce, and meeting any review and evaluation requirements specific to The Cyber Trust's industry and organisation type.

Staff Members' Responsibilities

23. All Staff Members are responsible for promoting the safety and well-being of all of The Cyber Trust's Beneficiaries by following all of The Cyber Trust's policies and procedures relevant to safeguarding and all UK laws relevant to safeguarding. Specifically:

a. All Staff Members at The Cyber Trust play a role in keeping Beneficiaries safe and every role will be covered in detail during training. In case of doubt, it is important to contact Dr Robert Nowill to clarify any aspect of roles and responsibilities.

b. Encourage all Staff Members to actively participate and ask questions if anything is unclear to Dr Robert Nowill.

c. Do not risk the safety or well-being of any of The Cyber Trust's Beneficiaries by avoiding any of the next situations:

i. Subjecting them to or facilitating abuse of any sort.

ii. Engaging in any sexual activity with children (i.e. anybody under the age of 18).

iii. Participating in or facilitating any activities that may commercially exploit Beneficiaries. For example, failing to report suspected child labour or trafficking.

d. Staff Members must report all Safeguarding Concerns that they have regarding Beneficiaries' safety, regardless of whether the concerns relate to potential wrongdoing of other Staff Members, other Beneficiaries, or external parties (e.g. parents, teachers, other organisations, or members of the public).

Procedures: Reporting

24. To ensure the safety of The Cyber Trust Beneficiaries, Staff Members will be trained to recognise potential safeguarding concerns like abuse, neglect, and threats to well-being.

25. Staff Members who identify a safeguarding concern should report it following the next steps:

a. Where any allegations or suspicions of abuse occur escalate immediately to the Designated Safeguarding Lead, Deputy Safeguarding Leads, Trustees, or to local police or local social services.

26. Staff Members unable to follow the standard reporting steps should still report the concern in another alternative way. This may be the case if, for example:

a. Contacting someone potentially involved in the concern, or someone the Staff Member feels uncomfortable approaching, or

b. In emergencies involving a risk of serious harm, contact emergency services (e.g. police, ambulance, mental health crisis line) directly, or, if appropriate, report the concern to a senior member of The Cyber Trust's staff.

Procedures: Investigation and Response

27. All Reported Safeguarding Concerns at The Cyber Trust are treated seriously and addressed promptly by trained personnel following the established procedures and relevant laws. For more details about these procedures, please contact Dr Robert Nowill.

28. We aim to keep Staff Members who report a Safeguarding Concern informed about its progress as much as possible, depending on the nature of the concern and the confidentiality of the investigations.

29. In case of breach of this Safeguarding Policy or safeguarding law in general by a Staff Member, they will be treated fairly and will only be dismissed if appropriate in the circumstances and in accordance with employment law.

30. External referrals or notifications (e.g. to police services, local authorities, or regulatory bodies) will only be made when deemed necessary and strictly following applicable laws, including data protection regulations, to ensure the safety and well-being of Beneficiaries.

Supporting Documents and Other Protections

31. Other documents that support The Cyber Trust's Safeguarding Policy:

a. Safeguarding Code of Conduct

32. Contact the person within the Organisation responsible for HR matters or Staff Members' line managers to obtain this policy, along with related procedures and documents.