UK CYBER SECURITY COUNCIL

TRUSTEE REPORT
AND FINANCIAL STATEMENTS
FOR THE YEAR ENDED 31 MARCH 2022

Company Number: 12830814
Charity Number: 1195030
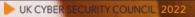
FIND MORE **UKCYBERSECURITYCOUNCIL.ORG.UK**

CONTENTS

2 – 20 Trustee Report

FOREWORD FROM OUR CEO

This is our first retrospective of our accomplishments since the charity was formed in April 2021, and of our partnership working with the formation team led by the IET, the industry, DCMS, and since September, with our new members!

I am hugely proud of how far we have come over the last nine-months and all the contributors to our story, from the original four Board Directors who led us from inception, through the start-up process and into on-boarding members, under the experienced leadership of Dr Claudia Natanson. The four new Directors who have added so much more fullness to our Board and are already making their mark on the future of the organisation. And of course, my team, who have been so adaptable, dependable and innovative in responding to the needs of a new enterprise, evolving requirements and strategies. I have been humbled by their collective enterprise, and to them all, a huge thank you!

From my initial days, I have sought to develop the Council along four-core strategic aims.

- ▶ **Structure the council to deliver the UK Cyber Security Strategy**
- ▶ **Develop a sustainable & diverse workforce of cyber professionals**
- ▶ **Engage with & listen to industry**
- ▶ **Make every contact matter**

All decisions and actions have been driven by this agenda and I am extremely proud of the achievements my team are already making and the changes we are driving through the industry.

I have already noted how I have structured the Council to achieve Charitable Status, no mean feat.

We can now work with members and partners to have professionals in the industry able to become chartered for the first-time.

Speaking of members, we now have over 30 from across the industry, large and small, professional, not for profit and academic. These will be the 'life-blood' of the Council. Driving our thought-leadership agenda through volunteering on our committees, currently looking at Diversity and Inclusion, Industry Ethics and Career Mapping; all areas I am personally phenomenally passionate about, and I look forward to seeing their recommendations.

These engagements are continued in our upcoming series of roadshows where I will be out and about in the regions, further building our working relationships with our partners in all four nations and meeting our new members in person. As the world opens back up after the last two-years, I want to make sure that cyber security is front and centre.

Even through the various lockdowns, I, and my Board, have managed to be out and about, either virtually or in person.

I have held almost 100 strategic partnership meetings and met regularly with DCMS, NCSC and the Cabinet Office. For many, we are now the organisation to call should they need advice in our sector, and we consult regularly with government and beyond on their research and strategies.

There is much to be done and I look forward to leading it, but I am also delighted to take the opportunity of this Trustee Report to chronicle just how far we have already come.

Professor Simon Hepburn
Council Chief Executive Officer

PURPOSE AND PUBLIC BENEFIT

The purpose of the UK Cyber Security Council is to act as the voice of the cyber security profession and help ensure that the UK is the safest place to live and work online, as set out in the original National Cyber Security Strategy (2016-2021).

Its aims are to:

▶ Inspire, inform and advance public cyber security awareness and knowledge

▶ Create an open, inclusive and professional cyber security culture

▶ Influence cyber security best practices that proactively benefit the public in the UK and beyond

▶ Act as the reference point for cyber security professional standards, competence and commitment

We have established 5 pillars to deliver our aims, these pillars are:

▶ Professional Standards - Setting the standards for practitioners across the sector

▶ Professional Ethics - Creating and ensuring cyber professionals adhere to our Code of Ethics

▶ Careers & Learning - Providing guidance on how to join and progress within cyber security

▶ Outreach & Diversity - Striving for an inclusive and representative sector

▶ Thought Leadership & Influence - Positioning the Council as the voice of the profession

By bringing together professionals within the cyber security sector, with stakeholders, government, and third sector organisations, we will establish professional standards and ethics, alongside our work to encourage progression within the sector.

We will work in collaboration with the wider industry to tackle issues such as closing the skills gap and make sure we see a more representative workforce.

Public Benefit
One of our key values is inclusion. This means everyone. We embrace diversity of all kinds and the rich knowledge this empowers us with.

We break down barriers, promote fairness and champion the need and the benefits for inclusion.

We will benefit the public through our work to demystify and simplify career paths within cyber security, which will have a tangible impact through the reduction of the skills gap in the sector.

We will ensure those in the profession are working to a defined standard and code of ethics, and make sure anyone wanting to start a career in or progress within cyber security can.

This not only benefits individuals, but also employers, businesses, and the wider community; creating a world where the whole of society is safe and secure in cyber space.

BUILDING FORWARD: FUTURE STRATEGY

IMPACT

The UK has a world class and diverse cyber security sector, with expanded and enhanced skills at all levels

UKCSC VISION

The Cyber Security Council is established as the trusted voice for the sector

UK CYBER SECURITY COUNCIL

OUTCOMES

Strengthened dialogue between UKCSC member organisations

Cross-cutting: Thought Leadership

Coordination between private and public sector stakeholders promotes the cyber profession

Pillar 1: Standards

Employers and recruiters adopt sector-wide standards on cyber qualifications

Professionals build cyber skills and expertise to strengthen employment opportunities

Pillar 2: Ethics

UKCSC establishes and promotes a sector-wide code of ethics

Employers enhance monitoring and deterrence practices against abuse and unethical behaviour

Pillar 3: Careers / Learning

Professionals have increased awareness of pathways to entering and progressing in the sector

Employers and teachers increase training and mentorship opportunities

Pillar 4: Outreach / Diversity

Diversity of the sector increased with greater inclusion of underrepresented groups

Professional opportunities increased through expanded outreach by UKCSC

PROBLEM STATEMENT

Key problems: Poor diversity and inclusion within the UK cyber security industry; lack of universal professional and ethical standards; lack of consistency in vision across the sector; limited public awareness of professional opportunities; lack of universal qualifications or certifications.

ASSUMPTIONS

- Consistency in alignment with HMG policy and regulations
- Financial stability through diversified funding
- Stakeholder engagement remains strong
- Conducive professional environment for cyber employees
- External shocks or adverse disruptions remain manageable
- Continued participation of members and partners

YEAR IN REVIEW: FIRST HALF YEAR SUMMARY

The Council Formation Project ran for almost two years and was led by the Institute of Engineering Technology (IET) under the chair of Dr Budgie Dhanda MBE working in partnership with DCMS and several industry partners and industry volunteers, all now Founder Members of the Council.

The volume of work that came out of this project was considerable and covered all the key areas in the UK's Cyber Security Strategy. Most of this work has subsequently been taken forward into the GFA and the Council's own planning. Of the areas not fully developed, key were the business planning and financial sustainability.

The Formation Project defined four key strategic aims that sought to respond to the DCMS's original requirements in:

▶ **Professional Development**
▶ **Outreach & Diversity in Cyber Security to develop the next generation**
▶ **Professional Ethics**
▶ **Thought Leadership & Influence**

These aims have now been subsumed into the Council's four strategic aims.

▶ **Structure the council to deliver for the UK Cyber Security Strategy**
▶ **Develop a sustainable & diverse workforce of cyber professionals**
▶ **Engage with & listen to industry**
▶ **Make every contact matter**

Which have then been augmented by the specific requirements of the DCMS Grant Funding Agreements, the second of which is due to be entered into early in 2022-23.

Through the first six months of this financial year, the Council put in-place its Phase One Strategy, focused upon the evolution from the Formation Project to a live organisation.

There were six aims in all driven by an interim MD with the initial four Board Trustees.

▶ **Successfully launch brand & build positive presence**
▶ **Launch and on-board initial members positively with a clear role (Phase One)**
▶ **Secure successful relationships with government and be seen to 'add value' and be the first point of call at all levels**
▶ **Develop new business areas of potential income**
▶ **Establish all management functions and secure the team**
▶ **Prepare for phase two**

This Phase One Strategy was treated as a project, fully programmed, baselined and tracked, with specific outcomes to be achieved and KPIs presented in a balanced scorecard format to the board and DCMS.

.

YEAR IN REVIEW: SECOND HALF YEAR SUMMARY

Into the second half of the year, Simon was appointed with all the knowledge and experience he brings to the role. With the business established, workstreams underway and the remaining Board posts filled, the Council was able to begin to focus on its deliverables under the DCMS GFA and the Board's wider ambitions for the organisation's role in the sector.

The CEO was quick to structure the work for the second half of the year around four key pillars:

Develop a sustainable workforce of cyber professionals

We will work with our partners in government, industry and academia to improve the expectations of the chartered/registered cyber security professional. We will develop understandable career pathways, coupled with accredited qualifications to achieve recognised career levels within the profession. We will do this in a manner that is fair, open and transparent, keeping our requirements and guidance relevant, effective, and representative of individuals' diverse requirements.

Engage with & listen to industry

We will continue to listen to the industry about the support it requires and its expectations of the chartered/registered cyber professional. We will continue to develop our work with industry partners to facilitate working committees on key cyber security and industry issues and ensure the findings are well understood across the industry and government.

Make every contact matter

We will treat every contact with every person and organisation as an opportunity to promote the work of the Council, the UK's Cyber Security Strategy, to promote the industry, our members, the profession and professionals.

All types and forms of contact and contact points will be treated as opportunities for positive engagement and for learning.

Structure the council to deliver the UK Cyber Strategy

We will structure the Council to deliver the ambitions of DCMS, the industry and our members and ensure each area of work receives the resources it requires to be successful. We will put processes in place to develop our staff into key roles, creating a culture of positive leadership in an organisation that is innovative, professional and forward looking.

YEAR IN REVIEW: ACHIEVEMENTS

Develop a sustainable workforce of cyber professionals

UK CYBER SECURITY COUNCIL **2022**

TRUSTEE REPORT FOR THE YEAR ENDED 31 MARCH 2022

YEAR IN REVIEW: ACHIEVEMENTS

Some key achievements under the pillar of 'develop a sustainable workforce of cyber professionals ' are as follows:

▶ Commenced phase 1 of mapping career choices & pathways through our industry. A free resource for any current or aspiring cyber professional at any point in their career

▶ Contributed & responded to the National Cyber Security Council's 'Decrypting Diversity' Report

▶ Commenced work on creating the charter specifications that are aligned to the cyber specialisms.

Digital Forensics

Cyber Threat Intelligence

Cyber Security Generalist

Cyber Security Management

Incident Response

Network Monitoring & Intrusion Detection

Vulnerability Management

Security Testing

The Careers Route Map: pathways for the 16 specialisms in cyber security.

Pick a specialism to find out more.

Cryptography & Communications Security

Secure Operations

Identity & Access Management

Secure System Architecture & Design

Cyber Security Audit & Assurance

Data Protection & Privacy

Secure System Development

Cyber Security Governance & Risk Management

YEAR IN REVIEW: ACHIEVEMENTS

Some key achievements under the pillar of 'engage and listen to the industry' are as follows:

▶ On-boarded over 30 new members from across the industry

▶ Delivered our 'spotlight on' series. An opportunity for professionals to learn from others

▶ Implemented the first of our thought leadership committees, Standards and Careers.

▶ Led a series of workshops for and with industry, with the Department for Digital, Culture, Media and Sport (DCMS) to engage with the pathways and careers consultation.

▶ Planned and delivered high profile events including a celebration of women in cyber event to celebrate International Women's Day and a finance symposium for finance and cyber leaders.

Engage and listen to industry

In addition to this there are some areas highlighted in the next section that overlap with this pillar.

YEAR IN REVIEW: ACHIEVEMENTS

Some key achievements under the pillar of 'make every contact count' are as follows;

▶ Strategic meetings with over 100 sector leaders to inform the development of the Council and our work

▶ Planned a UK-wide roadshow for the first quarter of 2022 to sense-check our work on standards, ethics, careers and qualifications

▶ Established a regular presence in industry & business media including in City AM, Computer Weekly, CSO Online and InfoSecurity Magazine

▶ Built positive working relationships with all devolved administrations in Scotland, Wales and Northern Ireland

▶ Became a formal member of the CyBOK (Cyber Body of Knowledge) Steering Committee

▶ Nearly 120,000 views on posts on LinkedIn and other social media channels

▶ Presented or spoke at events including those run by the Department for Digital, Culture, Media and Sport (DCMS), the National Cyber Security Centre (NCSC), The Security Institute, The Security Awareness Special Interest Group (SASIG) and The Chartered Society of Forensic Sciences

Make every contact matter

YEAR IN REVIEW: ACHIEVEMENTS

Structure the council to deliver on UK Cyber Security Strategy

▶ **Some key achievements under the pillar of 'structure the Council to deliver on the UK Cyber Security Strategy' are as follows:**

▶ Secured an industry-leading Chair in Dr. Claudia Natanson MBE

▶ On-boarded a further seven high calibre experienced Board Trustees from our industry & beyond

▶ Secured Simon Hepburn as our first CEO, a charity and education executive with over twenty years' experience in a variety of national and international organisations

▶ Built a dedicated & industrious team to deliver for the Council & the Industry

▶ Established our governance arrangements, including sub-committees & thought workshops

▶ Launched our organisational membership programme and exceeded our full financial year target

▶ Secured three-year funding from DCMS

REFERENCE & ADMINISTRATION:

Company Number: 12830814

Charity Number: 1195030

Registered Address: 3rd Floor, 106 Leadenhall Street, London, EC3A 4AA

Bankers:

Lloyds Bank PLC. 25 Gresham Street, London EC2V 7HN

Co-operative Bank PLC. PO Box 101, 1 Balloon Street, Manchester, M60 4EP

Solicitors:

Birkett's LLP. Providence House 141-145 Princes Street, Ipswich, Suffolk, IP1 1QJ

Auditors:

Moore Kingston Smith, 9 Appold Street London EC2A 2AP

Trustees:

▶ Claudia Natanson - Chair (appointed October 2020)

▶ Jessica Figueras – Vice Chair (appointed October 2020)

▶ Mike Watson – Treasurer (appointed October 2020)

▶ Carla Baker – Trustee (appointed October 2020)

▶ Chitra Balakrishna – Trustee (appointed October 2021)

▶ Nathan Nagaiah – Trustee (appointed October 2021)

▶ Edward Goodchild – Trustee (appointed October 2021)

▶ Frances Le Grys – Trustee (appointed October 2021)

The UK Cyber Security Council was incorporated as a company limited by guarantee on 21 August 2020.

The UK Cyber Security Council was registered as a Charity on 01 July 2021.

RESERVES POLICY

The Trustees treat the unrestricted reserves as available for activities which forward the Charities objectives, and for funding the requirements for support and governance costs.

Free reserves are that part of the Council's unrestricted funds that are freely available to spend on any of its charitable purposes.

The Council may maintain free unrestricted reserves for the following reasons:

a) to provide a level of working capital that protects the continuity;

b) to provide a level of funding for unexpected opportunities; and

c) Forman tc provide cover for risks such as unforeseen expenditure or unanticipated loss of income.

The Trustees will review the above criteria with reference to

the Council's strategy and Annual Plan and determine the

target level of free reserves to meet these.

They may at times designate funds from free reserves for

significant project costs or replacement of major assets.

RISK MANAGEMENT

The UK Cyber Security Council Trustees have considered the major risks to which the charity is exposed and have reviewed those risks and established policies, systems and procedures to manage them accordingly.

The risk register is updated at least quarterly, but is regularly reviewed within the operational team to ensure key changes are reflected in the risk log and appropriate plans to mitigate are put in place.

The principal risks are:

• Loss of funding or inability to secure sufficient funding to carry out the core work of the organisation

• Significant delays in the development and roll out of specialist cyber standards

• Breach of data security or compliance with key regulatory authorities

• Loss of key staff and personnel

• Lack of support and buy in from the cyber security profession

GOVERNANCE STRUCTURE

The Council was conceived initially as part of the UK Government's National Cyber Security Strategy, which set out ambitions to develop and accredit the cyber security profession. It seeks to do this by "reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy."

This was developed further in the Initial National Cyber Security Skills Strategy (2018). This declared intentions to establish a new, independent, UK Cyber Security Council to act as an umbrella body for existing professional organisations and drive progress against the key challenges the profession faces.

Following a competitive tender process, the Department for Digital, Culture, Media and Sport (DCMS) awarded the contract to design and deliver the Council in September 2019 to a consortium of cyber security professional bodies known as the Cyber Security Alliance.

The first four Trustees were appointed by the Cyber Security Alliance in October 2020. The Board expanded to 8 Trustees in October 2021, with the four new Trustees appointed by the Board, in conjunction with the Interim Chief Executive. Four places remain available on the Board, and will be appointed by the Council's member organisations, with the first two elected Trustees taking up post in October 2022.

Our Board of Trustees has a broad range of relevant skills, knowledge and experience, spanning education, skills and professional development, commercial and business development, income generation and fundraising, legal, cyber security, financial management, risk management, business risk, professional standards and ethics, Government affairs and policy and furthering diversity, equality and inclusion.

The Council considers each of the Trustees independent in character and judgement.

Declarations of interest are acquired from new Trustees and updated by all trustees annually. No remuneration is provided other than reasonable travel and subsistence costs. Trustees regularly review the progress of the charity and its funding and work in conjunction with the executive team and membership bodies to set the strategy for the organisation.

Remuneration
The Chair reviews the remuneration of the Chief Executive and makes a recommendation to the Remuneration Committee for consideration. The Remuneration Committee also review the salaries of the Leadership Team.

Auditors
The Board of Trustees approved the appointment of Moore Kingston Smith as the Auditors on 23/3/22

The Council are governed by our Articles of Association (as a Charity Body)

There are a maximum of 12 Trustee spaces; 10 spaces are currently taken - 8 by general appointment, 2 appointed by the membership.

The Trustees are also responsible for the appointment of the Chief Executive, to which they delegate the day-to-day running of the Charity.

The Board has 4 sub-committees.

▶ The Programme Board ensures the Council's programme directorate activity including standards development and career route mapping is fit for purpose and in line with strategy and priorities of the organisation.

▶ The Finance and Audit Board review the risks, controls, and financial management of the organisation.

▶ The Remuneration Committee provides a forum, independent of the Council's other governance bodies, for the review and approval of the remuneration of the Chief Executive, the Leadership Team, and any ex-gratia payments.

▶ The Governance and Nominations Sub-Committee ensures the Council's governance is fit for purpose and that it is populated by suitably diverse and skilled individuals, in line with strategy and representation.

ORGANISATION STRUCTURE AND MANAGEMENT

As a start up organisation it is important that the operational and management structure of the organisation is fit for purpose to deliver on the Council's mission and objectives.

As such the Leadership Team working with the Human Resource Partner, review where there are any pinch points within the organisation and then seek to mitigate this through increased human resource or re-prioritisation of tasks.

This along with the development and implementation of new systems and processes helps staff to be more effective and efficient.

Our updated structure is made up of four directorates

▶ The Standards Directorate
Led by the Director of Professional Standards, this directorate is focussed on developing the professional standards based upon our 16 cyber specialisms.

▶ The Programme Directorate
Led by the Director of Programmes and Partnerships, this directorate is focussed on developing the careers road map, outreach programmes and the transition of programmes to the Council.

▶ The Finance & Ops Directorate
Led by the Director of Finance and Operations, this directorate is focussed on managing areas including the organisations finance, marketing, membership and events.

▶ The Chief Executives Office
Led by the CEO, this directorate is focussed on strategic planning, technical cyber, governance, external engagement and government relationships

In the 2023/2024 financial year we will be enacting the incorporation of our Royal Chartership, which in practical terms will mean the closure of the current charity and company incorporations, and transition to the new Chartered Charity and Organisation.

All contracted staff will be transferred over to the new organisation as part of this process.

FUTURE PLANS

The 2022-23 financial year will be the first year of delivering against our new strategy plan 'Chartering a Cyber Future', which was released in October 2022.

Our core focus in on the development and the **design of schemes that award professional titles** for the specialist areas representing the cyber security lifecycle, producing an agreed standard for Chartered, Principal and Associate.

To support this, our additional priorities are to:

▶ Raise the profile of the cyber security profession and the UK Cyber Security Council

▶ Develop an ethical framework in which the cyber security profession should operate

▶ Create cyber skills frameworks that are linked to the mapping of certifications and qualifications within the sector

▶ Carry out outreach activities to address the long-term skills gap in the sector

▶ Produce thought leadership pieces based on engagement with academia, members and other key stakeholders

▶ Establish the Royal Incorporated organisation to deliver on our mission

TRUSTEE ROLE, APPOINTMENT & INDUCTION

The role of a Trustee is to ensure that the Council fulfils its duty to its beneficiaries and delivers its vision, mission and values. Working together with the other Trustees – and in collaboration with the CEO they are instrumental in ensuring that the Council delivers its charitable objectives, and values equality, diversity and inclusion.

Our Trustees are individuals who have a strong empathy with our vision and mission combined with an in-depth understanding of our work and ambitions and they possess an understanding of the culture and needs of a values-driven organisation.

The role is one of legal liability and responsibility for the compliant running of a charity. Across the Board we seek skills and experience in running a professional organisation, although recognise that not all candidates will have these skills initially.

Trustees are legally required to act in the best interests of the Council and candidates should therefore not seek to influence the Board in terms of representing any other organisation.

For all Trustees, the following core skills are essential to undertake their duties:

- Excellent communication and influencing skills to be a strong ambassador for the Council

- A collaborative approach and openness to other views and feedback on own contribution

- An ability to think diversely, produce innovative ideas and challenge existing thinking and perspectives

- Commitment to the Council's mission and values

- Commitment to delivering public good

- Commitment to bringing high standards of ethics and transparency to the Council's governance

- Commitment to inclusion and diversity

Appointment of trustees

As set out in the articles of association, the board of trustees comprises

- not more than 12 trustees as Board Members
- Maximum of 4 elected from among and by the full members
- the chief executive of the Association as an ex-officio member of the Board
- Board members may serve up to two terms of three years

Trustees' induction and training

On appointment, new trustees are provided with information about the company including its constitution, strategy and plans, finances, staffing structure and its risk register.

Their attention is drawn to relevant Charity Commission guidance. They are offered the opportunity to meet with the chief executive and other staff for a full briefing on the organisation's work.

Organisation

The Board is responsible for the governance of the charity. The trustees delegate the running of the organisation to the chief executive, within a framework of delegated authority. The board meets at least quarterly.

YEAR IN REVIEW: FINANCIAL PERFORMANCE

Our first operating year was largely funded via a Grant Funding Agreement with the DCMS agreed in April 2021 with other income streams to be developed as the year progressed, to include membership levies, sponsorship and running of events.

Income

Overall income was £1,606 K comprised of £1,577 K from the DCMS Grant Funding Agreement and £29 K from new membership levies. A small amount (<£1 K) was also raised from speaking at events.

The Grant Funding Agreement had a funding ceiling of £1,581 K meaning the Charity underclaimed by just £4 K or 0.25%.

Expenditure

Total expenditure for the year was £1,539 k which was almost entirely spent on delivering against the DCMS's Grant Funding Agreement.

To be noted, is the impact of our VAT structure that meant a total of £214 K was spent and not reclaimable on VAT. This structure remains in-place but a review of this is on the agenda.

Cashflow

Cashflow at commencement was supported by several of our contractors and interim staff deferring their payments for the first three months, this enabled the Council to move forwards with its agenda without working capital and we are grateful to all of them for their contributions.

The Charity made a small surplus of £68 k at the year end. Total funds were £68 k with £14 k restricted and £ £54 k unrestricted in the first year of activity.

We are working with DCMS to ensure a three-month cover for total organisational expenses always remains in-place.

Into 2022-23

The DCMS have agreed a new Grant Funding Agreement that will provide income of up to £1,500 K to deliver against the contract KPIs.

Additionally, we expect to continue to on-board new members and see an increase in the total annual levies.

2022-23 will also be our first year of issuing Charterships to industry professionals and we will see substantive income against the delivery of the same.

Finally, our strategy for the coming years will ensure the financial sustainability of the organisation and develop appropriate additional income streams.

YEAR IN REVIEW: FINANCIAL PERFORMANCE

The UK Cyber Security Council's year ending Mar 2021 was the first year of activity for the charity.

Funded by the Department for Digital, Culture, Media & Sport (DCMS), the Council was able to:

- Recruit a board of Trustees
- Establish a governance structure
- Recruit its first employees, including a CEO
- Launch its website
- Engage and consult with stakeholders to inform the standard
- Launch its membership offering

This year was about establishing the core infrastructure, systems, and policies to enable the organisation to progress into our delivery phase.

The membership proposition, launched in October 2021, enables the council to recognise £28,958 of unrestricted income in the financial year, beginning the journey of financial sustainability for the council.

TRUSTEE STATEMENT OF RESPONSIBILITIES

The Trustees (who are also Directors of the UK Cyber Security Council for the purpose of company law) are responsible for preparing the trustee's report and financial statements in accordance with applicable law and United Kingdom accounting practices.

Company and Charity law requires the Trustees to prepare financial statements for each financial year.

Under company law the Trustees must not approve the financial statements unless they are satisfied that they give a true and fair view of the situation of the charitable company and of the incoming resources and application of resources, including the income and expenditure for that period.

The Trustees are responsible for keeping adequate and proper accounting records that are sufficient to show and explain the charitable company's transactions and disclose with reasonable accuracy at any time the financial position of the charitable company.

In preparing these financial statements, the Trustees are required to:

▶ Select suitable accounting policies and then apply them consistently

▶ Observe the methods and principles in the Charities SORP

▶ Make judgements and estimates that are reasonable and prudent

▶ State whether applicable UK accounting standards have been followed, subject to any material departures disclosed and explained in the financial statements; and

▶ Prepare the financial statements on the going concern basis unless it is inappropriate to presume the charity will continue in operation

They are also responsible for ensuring that the financial statements comply with the Companies act 2006.

As well as safeguarding the assets of the charitable company and group and hence for taking reasonable steps for the prevention and detection of fraud and other irregularities.

In so far as we are aware:

▶ There is no relevant audit information of which the charities auditor is unaware; and

▶ The Trustees have taken all steps that they ought to have taken to make themselves aware of any relevant audit information and to establish that the auditor is aware of that information.

The Trustees are responsible for the maintenance and integrity of the corporate and financial information included on the charitable company's website.

Legislation in the United Kingdom governing the preparation and dissemination of financial statements may differ from legislation in other jurisdictions.

The financial statements have been prepared in accordance with the special provisions of part 15 of the companies act 2006 relating to small companies.

Approved and signed on behalf of the Trustees by

**Dr Claudia Natanson MBE
Chair of Trustees**

13 December 2022