

AI and Cybersecurity in Conservation Charities

Turning technological change into greater impact—without increasing organisational risk

Executive Summary by
James Gittins

0800 099 6224

info@kynaassociates.com

www.kynaassociates.com

Artificial intelligence presents a major opportunity for conservation charities. Used effectively, it can help organisations identify funding opportunities, strengthen grant applications, improve supporter engagement, expand membership, analyse environmental data, automate administration and direct limited resources towards the activities that create the greatest impact.

For organisations operating under sustained financial pressure, AI could release staff from repetitive work and enable them to spend more time on conservation delivery, fundraising, partnerships and public engagement.

However, AI adoption also introduces significant risks.

Cybercriminals are already using AI to create more convincing phishing messages, impersonate senior leaders and suppliers, automate reconnaissance and scale attacks. At the same time, employees and volunteers may unknowingly expose confidential information by entering donor, supporter, employee or ecological data into public AI tools.

The challenge for conservation charities is therefore not whether to adopt AI, but **how to adopt it responsibly, securely and strategically**.

This report explores the principal opportunities, threats and governance priorities for conservation organisations seeking to benefit from AI while protecting their people supporters, data and reputation.

Part One – AI Opportunities for Conservation Charities

1. Why AI Matters to the Conservation Sector

The operational pressures facing conservation charities and why AI has become strategically important.

2. Finding More Grant Funding

Using AI to identify funding opportunities, monitor grants and improve funding success.

3. Producing Stronger Grant Applications

How AI can support bid writing while retaining human expertise.

4. Growing Membership and Supporter Engagement

Using AI to improve donor communications, membership growth and supporter retention.

5. More Effective Marketing and Campaigning

Creating better campaigns, content and public engagement with fewer resources.

6. Environmental Monitoring and Conservation Delivery

Applying AI to biodiversity monitoring, habitat analysis, camera traps, drones and ecological data.

7. Volunteer Recruitment and Management

Improving volunteer recruitment, onboarding, communication and retention.

8. Reducing Administrative Workloads

Automating repetitive tasks so staff can focus on higher-value conservation work.

9. Better Leadership Decision-Making

Using organisational data to improve strategic planning and operational decisions.

Part Two – AI and Cyber Security Risks

10. Why People Remain the Greatest Cyber Risk

Reducing human error through awareness, training and culture.

Part Three – A Practical Framework for Responsible AI Adoption

11. AI-Powered Phishing and Impersonation

Understanding how attackers are using AI to create more convincing cyber attacks.

12. Deepfake Voice and Video Fraud

Preparing for emerging AI-enabled impersonation threats.

13. Protecting Confidential Information

Managing the risks of employees entering sensitive data into public AI tools.

14. AI Hallucinations and Inaccurate Information

Why AI-generated content always requires expert review.

15. Bias and Automated Decision-Making

Understanding fairness, accountability and responsible use of AI.

16. Protecting Public Trust

Maintaining confidence among donors, members and stakeholders.

17. Managing an Expanding Attack Surface

Understanding the security implications of adopting new AI technologies.

18. Shadow AI

How unmanaged AI usage creates hidden organisational risks.

19. The Environmental Cost of AI

Balancing innovation with environmental responsibility.

20. Start with Organisational Needs

Identifying where AI can deliver the greatest value.

21. Developing an AI Policy

Creating clear governance, acceptable use and accountability.

22. Data Classification

Defining what information can—and cannot—be used with AI.

23. Training Employees, Trustees and Volunteers

Building organisational capability and resilience.

24. Strengthening Core Cyber Security Controls

The essential foundations every charity should have in place.

25. Pilot Before You Scale

Implementing AI safely through measured, low-risk pilot projects.



Responsible AI as a Force Multiplier for Conservation

How conservation charities can increase capacity, strengthen cyber resilience and deliver greater environmental impact through secure, well-governed AI adoption.

1. Why AI matters to the conservation charity sector

Conservation charities operate in a particularly demanding environment. Many manage large numbers of members, donors and volunteers while also running nature reserves, visitor centres, research programmes, advocacy campaigns and community projects.

Their teams are often geographically dispersed. Employees and volunteers may work from reserves, home offices, regional centres and shared facilities. Information may be held across membership platforms, fundraising databases, cloud applications, geographic information systems, scientific datasets and third-party supplier platforms.

At the same time, many organisations face:

- Increasing competition for grants and donations.
- Rising operational costs.
- Pressure to demonstrate measurable environmental impact.
- Limited digital and technology capacity.
- Growing expectations from supporters.
- Increasingly sophisticated cyber threats.
-

AI can help address several of these pressures—but only where adoption is tied to clear organisational objectives.

The Charity Commission has recognised both sides of this issue: AI can free charities from resource-intensive administrative work, while introducing legal, ethical and governance risks, particularly where it influences organisational decisions.

The opportunities

2. Finding more grant-funding opportunities

One of the most immediate uses of AI is improving the way conservation charities identify potential funders.

Funding teams often spend substantial amounts of time searching grant databases, monitoring trusts and foundations, checking eligibility criteria and matching opportunities to projects.

AI-enabled systems can help organisations:

- Search and categorise large numbers of funding opportunities.
- Match grants to specific conservation programmes.
- Track application deadlines.
- Identify newly launched funds.
- Analyse previous funding patterns.

- Flag opportunities linked to biodiversity, climate, heritage, education or community engagement.
- Prioritise applications according to likely fit and potential value.

A conservation charity could, for example, use AI to match a habitat-restoration programme against funds supporting biodiversity recovery, climate resilience, nature-based solutions, community participation and environmental education.

This does not replace experienced fundraisers. It gives them a faster and more systematic way to identify where their time is most likely to produce results.

3. Producing stronger grant applications

Generative AI can support the early drafting and structuring of funding applications.

It can help teams:

- Interpret funder criteria.
- Build an initial application structure.
- Summarise project plans and supporting evidence.
- Translate technical conservation language into accessible outcomes.
- Check whether each application question has been addressed.
- Adapt an existing case for support to different funder requirements.
- Improve clarity, consistency and grammar.
- Create first drafts of monitoring and evaluation frameworks.

AI can also help convert scientific or operational information into outcomes that funders can understand—for example:

- Hectares of habitat restored.
- Species populations monitored.
- Volunteers trained.
- Communities engaged.
- Carbon stored or emissions avoided.
- Improvements in water quality.
- Increased public access to nature.

Charity-sector guidance already identifies automated proposal drafting as a practical AI opportunity, but generic AI-generated applications can be weak or unsuccessful when they fail to reflect an organisation's actual work. Human evidence, judgement and specificity remain essential.

The best use of AI is therefore as a **research and drafting assistant**, not as an autonomous bid writer.

4. Improving supporter engagement and membership growth

Many conservation charities hold significant information about members, donors, volunteers, event attendees, campaign supporters and website visitors.

AI can help analyse this data to identify:

- Which communications generate the strongest engagement.
- Which supporters are most likely to become members.
- Which members may be at risk of lapsing.
- Which campaigns generate donations or volunteer action.
- Which subjects resonate with different audiences.
- The most effective time and channel for communication.
- Potential major donors or legacy supporters.
- Opportunities for cross-selling membership, events, volunteering and appeals.

AI-powered segmentation can enable charities to move beyond broad, identical communications and create more relevant supporter journeys.

For example, a supporter interested in local wetlands could receive content about reserve restoration, bird surveys and volunteering opportunities, while another interested in marine conservation might receive material about coastal species, plastic pollution or citizen-science programmes.

This should improve engagement without simply increasing the volume of communications.

AI can also support accessibility through automatic captioning, transcription, translation and simplified-language versions of content, helping conservation organisations reach broader and more diverse audiences.

5. More effective marketing and campaigning

Conservation charities frequently need to communicate complex issues to the public.

AI can support marketing teams by helping them:

- Produce campaign concepts and content variations.
- Repurpose reports into articles, newsletters and social posts.
- Summarise scientific research for public audiences.
- Create personalised supporter communications.
- Analyse the performance of previous campaigns.
- Monitor public sentiment.
- Identify emerging environmental conversations.
- Test different headlines and calls to action.
- Improve search visibility and website content.
- Produce accessible versions of technical information.

It could allow a small communications team to turn one detailed conservation report into:

- A member email.
- A press release.
- A short social campaign.
- A trustee briefing.
- A volunteer update.
- Educational material.
- A local authority briefing.
- A donor impact report.

The benefit is not simply producing more content. It is creating relevant content more efficiently and making expert knowledge available to different audiences.

However, output must remain fact-checked. Inaccurate statements about species, habitats, planning policy or scientific findings could damage public trust.

6. Environmental monitoring and conservation delivery

AI has applications far beyond administration and marketing.

It can help conservation practitioners analyse information from:

- Camera traps.
- Acoustic sensors.
- Satellite imagery.
- Drones.
- Geographic information systems.
- Water-quality sensors.
- Species records.
- Citizen-science submissions.
- Remote monitoring equipment.

Potential uses include:

- Recognising species in images.
- Identifying birds, bats, insects or marine mammals from sound.
- Detecting changes in habitats.
- Monitoring invasive species.
- Identifying illegal deforestation or land-use change.
- Predicting wildfire, flooding or erosion risk.
- Prioritising areas for restoration.
- Detecting anomalies in environmental datasets.
- Improving the speed of biodiversity assessment.

UNESCO notes that conservation projects are increasingly combining AI with satellite imagery, camera traps and acoustic monitoring to understand biodiversity trends and inform conservation activity.

This could allow organisations to monitor larger areas more frequently and direct scarce field resources towards the locations that need intervention most.

AI should not replace ecologists, rangers or local knowledge. Its strongest role is to help experts analyse larger volumes of information and make better-informed decisions.

7. Volunteer recruitment and management

Volunteers are fundamental to many conservation organisations, but recruitment, coordination and retention can be administratively demanding.

AI could help charities:

- Match volunteers to suitable roles.
- Identify skills within volunteer databases.
- Automate routine onboarding communications.
- Personalise training material.
- Predict where volunteer shortages may arise.
- Analyse why volunteers leave.
- Schedule activities more efficiently.
- Answer frequently asked questions.
- Translate instructions for a wider audience.

A well-designed AI assistant could help volunteers find local opportunities, understand what equipment they need and receive relevant safety or training information.

However, automated decisions should not exclude people unfairly, and volunteers should always have access to a person where decisions or personal circumstances are involved.

8. Reducing administrative pressure

Many employees in charities spend substantial time on low-value but necessary administration.

AI can support:

- Meeting summaries and action lists.
- First drafts of reports.
- Policy research.
- Document classification.
- Data entry.
- Contract and supplier summaries.
- Internal knowledge searches.
- Trustee-paper preparation.
- Frequently asked questions.
- Event administration.
- Training content.
- Routine email correspondence.

The opportunity is to release time for work that requires human empathy, creativity, relationships, scientific expertise and judgement.

For a small conservation charity, even modest productivity gains across fundraising, operations, membership and communications could be significant.

9. Better organisational decision-making

AI can help leadership teams identify patterns that are difficult to see when information is distributed across departments and systems.

Potential examples include:

- Comparing fundraising performance with campaign activity.
- Identifying membership trends by geography.
- Measuring the impact of reserve events on supporter recruitment.
- Forecasting income.
- Modelling the effect of different subscription prices.
- Understanding volunteer retention.
- Analysing project costs and outcomes.
- Highlighting underused assets or facilities.
- Prioritising investment across sites.

Used well, AI can support evidence-based decisions. Used poorly, it can produce misleading conclusions based on incomplete, biased or inaccurate data.

The quality of the answer will depend heavily on the quality and relevance of the underlying information.

Part Two: The risks and threats

10. Employees and volunteers remain a major point of vulnerability

Technology alone does not create security.

Most cyberattacks still rely on persuading or deceiving a person into doing something:

- Opening a malicious attachment.
- Clicking a fraudulent link.
- Disclosing a password.
- Approving a false payment.
- Sharing confidential information.
- Downloading unauthorised software.
- Ignoring a security warning.
- Reusing compromised credentials.

The UK Government's 2025/26 Cyber Security Breaches Survey found that phishing was experienced by **25% of charities** and remained by far the most commonly identified cyber threat.

However, it is more productive to view people as part of the defence rather than simply describing them as the problem.

Staff and volunteers become a significant risk when they are:

- Poorly trained.
- Working under pressure.
- Using unmanaged devices.
- Given excessive system access.
- Unable to report mistakes safely.
- Exposed to confusing procedures.
- Using unsupported technology.
- Not informed about emerging threats.

A strong security culture turns employees into an early-warning system.

11. AI-generated phishing and impersonation

Generative AI allows criminals to produce convincing emails quickly, accurately and at scale.

Poor grammar and unusual wording were once useful indicators of a scam. AI can now generate professional messages that mimic:

- A chief executive.
- A trustee.
- A supplier.
- A funder.
- A local authority.
- A colleague.
- A bank.
- A technology provider.

Attackers can collect public information from websites, annual reports, job advertisements, LinkedIn profiles and social-media posts, then use it to create highly targeted communications.

A fraudulent email might refer to:

- A genuine conservation project.
- A real grant application.
- An upcoming trustee meeting.
- A supplier relationship.
- An event or public appeal.
- A named senior executive.

The NCSC expects AI to increase the scale and effectiveness of cyber operations, particularly by improving social engineering and helping less-skilled attackers conduct more capable attacks.

12. Deepfake voice and video fraud

AI can create convincing audio or video impersonations of senior staff.

A finance employee could receive what appears to be a call from the chief executive asking for an urgent payment. A supplier could receive a video message requesting a change of bank details.

A volunteer or regional employee could be manipulated by someone pretending to be a known colleague.

The NCSC has warned that AI-generated audio, video and identity documents are increasingly relevant to impersonation and identity fraud.

Conservation charities should therefore treat voice and video as supporting evidence—not definitive proof of identity.

High-risk requests should be verified through a second, trusted channel.

13. Confidential information entered into public AI systems

One of the most immediate internal risks is employees copying sensitive information into publicly available AI tools.

This could include:

- Donor and member records.
- Employee information.
- Volunteer details.
- Safeguarding information.
- Grant applications.
- Commercial contracts.
- Passwords or system configurations.
- Trustee papers.
- Unpublished scientific research.
- Locations of vulnerable species.
- Landowner details.
- Legal advice.
- Security incidents.

Once information has been entered into an external service, the charity may lose control over how it is processed, retained or accessed.

AI models and related systems can create data-protection implications, particularly where personal information is included. The ICO advises organisations to assess AI risks, establish a clear lawful purpose and use data-protection impact assessments where appropriate.

Every conservation charity should clearly state what information staff may—and may not—enter into AI tools.

14. Inaccurate or invented information

Generative AI can confidently produce information that is incomplete, misleading or entirely false.

For conservation organisations, this may include:

- Incorrect species information.
- Invented scientific references.
- Inaccurate ecological conclusions.
- Misquoted legislation.
- Incorrect grant criteria.
- False statistics.
- Non-existent funders.
- Misleading impact claims.
- Inaccurate planning-policy information.

This creates legal and reputational risks, particularly where content is published, submitted to funders or used to support environmental decisions.

AI-generated output should always be checked by someone with the relevant subject expertise.

15. Bias and unfair automated decisions

AI systems learn from existing information and may reproduce the bias, gaps and assumptions contained within it.

This matters where AI is used to:

- Screen job applicants.
- Select grant beneficiaries.
- Prioritise communities.
- Assess volunteers.
- Segment donors.
- Make funding decisions.
- Determine access to services.
- Evaluate employee performance.

A system may produce unequal outcomes even where no discrimination was intended.

Conservation organisations should be particularly cautious where automated decisions affect people, communities, employment or allocation of resources.

Human oversight and a clear route for challenge should remain mandatory.

16. Loss of public trust

Charities depend heavily on trust.

Members and donors expect organisations to protect their personal data, use funding responsibly and communicate truthfully.

Trust could be damaged if a charity:

- Publishes inaccurate AI-generated content.
- Uses synthetic images without disclosure.
- Suffers a donor-data breach.
- Automates sensitive supporter communications poorly.
- Uses AI to impersonate genuine human interaction.
- Makes unfair automated decisions.
- Is unable to explain how an AI system is being used.
- Overstates environmental results.

Transparency is therefore important.

Organisations should explain where AI materially influences a service, communication or decision, particularly where this could affect the expectations or rights of an individual.

17. Increased attack surface

Every new AI application creates another potential connection between users, organisational data, cloud platforms and external suppliers.

Risks may arise from:

- Weak access controls.
- Insecure integrations.
- Excessive permissions.
- Poor supplier security.
- Unpatched software.
- Compromised accounts.
- Misconfigured cloud services.
- Unauthorised employee tools.
- Plugins connected to internal databases.
- AI agents capable of taking actions autonomously.

AI tools should go through the same security, procurement and data-protection assessment as any other significant technology.

The NCSC emphasises that organisations integrating AI will still need strong fundamental security controls around the systems themselves and their dependencies.

18. Shadow AI

If organisations prohibit AI without providing guidance or approved alternatives, employees may simply use personal accounts or unauthorised tools.

This is sometimes described as **shadow AI**.

The organisation may then have no visibility of:

- What systems are being used.
- What data is being uploaded.
- Whether information is retained.
- Whether outputs are being checked.
- Which business processes depend on the tools.
- Whether suppliers meet UK data-protection requirements.

The answer is not a blanket ban. It is controlled adoption.

Charities should provide approved tools, clear rules, suitable training and a straightforward process for proposing new uses.

19. The environmental cost of AI

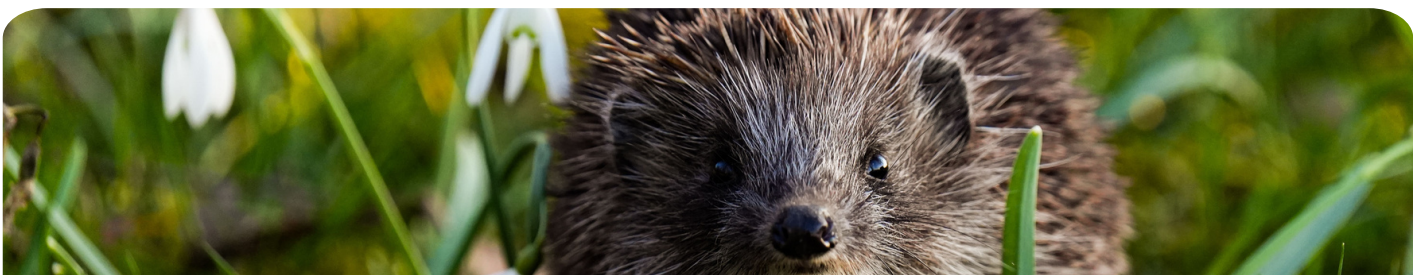
Conservation charities should also consider the environmental footprint of the technology itself.

Large-scale AI systems require computing infrastructure that consumes energy, water and physical resources. AI hardware also depends on mineral extraction and contributes to electronic waste.

This does not mean environmental organisations should reject AI. It means they should ask proportionate questions:

- Does this use of AI create measurable value?
- Could a simpler system perform the task?
- Is the supplier transparent about environmental impact?
- Are large models being used for small, routine activities?
- Can the organisation track usage and cost?
- Does the technology support—or undermine—the organisation's environmental commitments?

UNESCO describes AI as a double-edged environmental tool: it can improve conservation and environmental monitoring while also increasing energy, water, mineral and waste impacts.



Part Three: A responsible adoption framework

20. Start with organisational needs—not AI products

The wrong question is:

“Where can we use AI?”

The better question is:

“Which operational or conservation problems are consuming time, limiting income or reducing our impact?”

Priority areas might include:

- Grant research.
- Membership retention.
- Donor engagement.
- Biodiversity monitoring.
- Volunteer administration.
- Internal knowledge management.
- Campaign content.
- Data analysis.
- Reporting to trustees and funders.

Each proposed use should have a clear owner, objective and measure of success.

21. Establish an AI policy

Every organisation adopting AI should have a clear and practical policy covering:

- Approved AI tools.
- Prohibited information.
- Personal-data handling.
- Verification of outputs.
- Human oversight.
- Copyright and intellectual property.
- Acceptable use.
- Procurement and supplier checks.
- Transparency.
- Incident reporting.
- Employee and volunteer responsibilities.
- Review and accountability.

The policy should be short enough for people to understand and realistic enough for them to follow.

22. Create clear data classifications

Employees need to understand what information can be used in an AI system.

A simple classification model might include:

Public

Information already approved for publication, such as website copy, published annual reports and public campaign material.

Internal

Routine internal information that does not contain sensitive personal, commercial or ecological data.

Confidential

Employee records, donor information, contracts, unpublished research, financial information and internal strategies.

Highly sensitive

Safeguarding information, payment details, passwords, security information, legal advice and precise locations of endangered or vulnerable species.

Public AI tools should normally be restricted to public information unless a specific enterprise arrangement has been approved.

23. Train employees, trustees and volunteers

AI and cyber awareness should not be limited to the IT department.

Training should cover:

- Recognising sophisticated phishing.
- Verifying unusual payment or data requests.
- Deepfake and impersonation risks.
- Safe use of generative AI.
- Handling personal data.
- Reporting suspected incidents.
- Checking AI-generated content.
- Password management and multifactor authentication.
- Using approved devices and accounts.
- The organisation's AI policy.

Trustees and executives require additional training because they are both accountable for governance and attractive targets for impersonation.

24. Strengthen core cyber controls

AI does not remove the need for basic cyber hygiene.

Priority controls include:

- Multifactor authentication.
- Strong access management.
- Regular software updates.
- Secure backups.
- Tested incident-response plans.
- Managed devices.
- Email filtering.
- Password managers.
- Removal of dormant accounts.
- Supplier-security reviews.
- Segmentation of critical systems.
- Cybersecurity awareness training.
- Cyber Essentials or equivalent assurance.

The NCSC provides dedicated guidance and free tools for charities and smaller organisations, including support around backups, accounts, devices, phishing and incident exercises.

25. Pilot before scaling

AI adoption should begin with controlled, low-risk projects.

A pilot should:

1. Address a clearly defined problem.
2. Use non-sensitive information.
3. Involve a limited group of trained users.
4. Establish a baseline before implementation.
5. Measure time, cost, quality and risk.
6. Capture employee feedback.
7. Review data protection and security.
8. Decide whether the tool should be stopped, improved or expanded.

Examples of suitable early pilots include:

- Summarising public policy documents.
- Creating first drafts from already published material.
- Searching public grant opportunities.
- Categorising non-sensitive enquiries.
- Transcribing meetings with appropriate consent.
- Producing captions for public videos.

High-risk automated decision-making should come much later—if at all.

Conclusion



Artificial intelligence could become a powerful force multiplier for conservation charities.

It can help organisations find and secure more funding, engage supporters, expand membership, analyse environmental data and reduce administrative pressure. It could allow small teams to achieve work that previously required significantly greater time and resources.

But adoption without governance could expose those same organisations to data breaches, fraud, misinformation, regulatory risk and loss of public trust.

The distinction will not be between organisations that use AI and those that do not.

It will be between those that adopt it strategically—with the right leadership, skills and security—and those that allow it to spread informally without control.

For conservation charities, responsible AI adoption should therefore pursue three goals simultaneously:

Increase organisational capacity. Protect people and information. Deliver greater conservation impact.