Tech Secure Evaluation: Pilot to Support Digital Infrastructure in the Community and Voluntary Sector in Northern Ireland

July 2025

Prepared by

Dr Donna Kernaghan

Endorsed by

Contents

Figures and Tables	**P4**
Executive Summary	**P5**
Section 1: Background	**P10**
What is Tech Secure?	**P12**
Section 2: Results	**P16**
Stage 1: Digital Infrastructure Needs Assessment	**P17**
Case Study 1: A Small Charity's Digital Transformation	**P18**
Stage 2: Technical Implementation Results	**P18**
Stage 3: Tech Secure Staff Training Results	**P21**
Case Study 2: How Cyber Essentials Transformed a Youth Charity's Digital Security	**P22**
Case Study 3: How One Youth Work Charity Benefited from AI	**P27**
Conclusion	**P32**

Foreword

Digital is no longer an optional extra for the voluntary and community sector—it is the backbone of how we deliver services, safeguard people, and build trust in an increasingly complex world. Without secure systems, confident staff, and the right tools, organisations cannot achieve their full potential.

Northern Ireland's voluntary and community sector is one of our greatest assets. With more than 6,000 organisations, employing over 55,000 staff and supported by thousands of volunteers, it plays a vital role in tackling inequality, supporting communities, and delivering services where they are needed most. As the umbrella body for the sector, NICVA champions its voice, builds its capacity, and ensures organisations are equipped for the challenges ahead.

This report on the Tech Secure pilot matters because it goes beyond fixing immediate technical problems. It shows that systemic change is possible when expert partners are brought in not only to deliver solutions, but to embed skills, leave a legacy, and create sustainable change. The findings demonstrate that investment in digital infrastructure and training strengthens not just individual organisations, but the resilience of the sector as a whole.

The next step is to learn from this model and connect it to wider innovation ecosystems. Across health, education and business we see how strategic collaboration, long-term investment, and a culture of shared learning can accelerate transformation. The voluntary and community sector deserves the same. By scaling approaches like Tech Secure and linking them with other examples of innovation in Northern Ireland and beyond, we can build a sector that is digitally confident, resilient, and future-ready.

The potential is huge. With the right support, innovation and digital tools can free up capacity, unlock creativity, strengthen services, and open new ways of working with communities. This is about more than keeping pace—it is about giving the voluntary and community sector the means to thrive, adapt and lead in a digital age.

Celine McStravick

Chief Executive, NICVA

Figures and Tables

Figure 1: Participants' Self-Rating of Cybersecurity Skills After Tech Secure Training P21

Figure 2: Participants' Self-Rating of Digital Communication and Collaboration Skills After Tech Secure Training P24

Figure 3: Participants' Self-Rating of Data and Information Management Skills After Tech Secure Training P25

Figure 4: Participants' Self- Rating of Digital Tools After Tech Secure Training P26

Figure 5: Participants' Knowledge of IT Support After Tech Secure Training P27

Figure 6: Participants' Awareness of AI After Tech Secure Training P28

Figure 7: Participants Satisfaction with Tech Secure Training P31

Table 1: The Tech Secure Approach P13

Table 2: Technical Implementation Summary by Organisation P17

Table 3: Overall Impact of Tech Secure Training on Staff's Digital Skills P30

Executive Summary

The Bytes Project established Bytes Digital Innovation Ltd as a subsidiary to support the improvement of the digital infrastructure of the community and voluntary sector. Bytes Digital Innovation Ltd has a unique focus on charities supporting children and young people. During 2025, The Bytes Project, through its subsidiary Bytes Digital Innovation Ltd, secured funding from Innovate UK to develop the Tech Secure project which piloted support for four community and voluntary organisations to develop a solid and innovative cyber security ecosystem. Developed in partnership with Kero Business Solutions and Reconome, the project involved assessing current digital infrastructure, upgrading equipment and providing training to build staff knowledge and confidence in using digital tools to support their work with children and young people.

Stats & Stories was commissioned to evaluate the effectiveness and impact of the Tech Secure pilot in strengthening digital capacity among community and voluntary organisations. The evaluation combined data from the initial needs assessment conducted by Bytes Digital Innovation Ltd with pre- and post-training surveys completed by staff, alongside three qualitative interviews with representatives from participating organisations. This mixed-methods approach provided insight into both measurable outcomes and participants' experiences of the support received.

What is Tech Secure?

The Tech Secure pilot is a strategic initiative led by Bytes Digital Innovation Ltd, a social enterprise established by The Bytes Project to enhance the digital infrastructure of the community and voluntary sector.

The Tech Secure project was designed to support voluntary and community organisations working with children and young people in Northern Ireland to enhance their digital infrastructure, improve cybersecurity resilience and upskill staff. Specifically, Tech Secure aims to:

- Build digital capacity across the sector through tailored training and ongoing support;
- Enhance cyber security readiness and reduce risk exposure for voluntary organisations working with children and young people;

- Promote digital inclusion by ensuring access to up-to-date, secure devices and support;
- Support sustainability through a circular economy model and affordable, long-term service delivery.

Tech Secure Approach

The approach taken by Tech Secure ensured that participating organisations had both: (i) the technical infrastructure; and (ii) the skills base needed for long-term digital resilience and secure service delivery. This was conducted over three stages as outlined below.

Stage 1: Digital Infrastructure Needs Assessment Results

Bytes Digital Innovation Ltd conducted a comprehensive needs assessment to understand the organisation's digital skills and cybersecurity awareness. This involved surveys and interviews with staff to evaluate their current competencies and awareness of cybersecurity risks. In parallel, the organisation's cybersecurity infrastructure was audited, reviewing devices, software and existing practices to identify gaps and weaknesses.

The needs assessment revealed several critical security vulnerabilities across the participating organisations' IT infrastructure. Key issues included:

- the use of a consumer-grade router with default credentials which exposed the network to easy exploitation from hackers;
- multiple open ports accessible on the public IP, increasing the risk of remote attacks;
- the absence of network segmentation which allows potential attackers to move freely across the network if they gained initial access.

Stage 2: Technical Implementation Results

In order to remedy these critical issues uncovered by Stage 1, the Tech Secure project implemented a standardised technical stack across all participating organisations. This included successfully establishing Microsoft 365 tenancies, deploying managed endpoint security and implementing centralised user

management with multi-factor authentication across all participating organisations. This was key to ensuring consistency and enabling efficient management. The technical implementation aspect of the project achieved:

- 4 organisational Microsoft 365 Business Premium tenancies established and configured;
- 26 devices total upgraded to Windows 11 Pro with complete managed endpoint protection;
- 32 user accounts total deployed across all organisations with 100% Multi Factor Identification (MFA) implementation;
- Standardised security framework deployed across all participating organisations;
- 24/7 monitoring and automated patch management implemented uniformly.

Stage 3: Tech Secure Staff Training Results

Training delivered through the Tech Secure pilot led to marked improvements in digital confidence and capability across all six key skill areas. The evaluation methodology for the staff training element of the project followed a pre/post approach. Staff (n = 19) completed a pre-training survey to self-assess their skills across six key digital areas including cybersecurity and GDPR compliance, digital communication, data management, practical software skills, accessing IT support and an introduction to AI tools. After training, a subset (n = 11) completed a post-training survey using the same criteria. Results from the training across the six key digital skill areas included:

- **Cybersecurity and Data Protection:** Confidence rated as excellent or good increased from 63.1% pre-training to 100% post-training.
- **Digital Communication and Collaboration:** Improved from 84.2% to 100%, indicating full confidence across all participants after training.
- **Data and Information Management:** Increased from 68.4% to 100% after training showing strong gains in data handling and organisation skills.
- **Software and Digital Tools:** Confidence rose from 68.4% to 100%, reflecting better understanding and use of key tools.

- **Awareness of Accessing IT Support:** Grew from 68.8% to 90.9%, improving participants' ability to seek help when needed.
- **AI Awareness:** Increased from 66.7% to 91.0%, demonstrating participants' greater understanding of AI's relevance and potential.

Satisfaction with Training: The data indicates a high level of staff satisfaction with the training provided by Bytes Digital Innovation Ltd across all areas. All participants also rated the effectiveness of the overall training as very effective (81.8%) or effective (18.2%) with particularly strong responses for Data and Information Management and Digital Communication and Collaboration with 90.9% reporting being very satisfied.

Conclusion

The evidence suggests that the Tech Secure project has significant potential to help community and voluntary organisations tackle persistent challenges in establishing and managing their digital infrastructure. Common risks identified through the Tech Secure needs assessment process included absence of a managed IT infrastructure, vulnerability to hacking, lack of antivirus protection and use of inappropriate or outdated equipment and software. In addition, staff in participating organisations required training on data management, cybersecurity and troubleshooting to safeguard sensitive information and maintain system integrity. Staff also needed support to develop their own skills and knowledge on how to make better use of digital tools and boost productivity through AI.

The pilot directly addressed these challenges by supporting organisations to implement managed IT systems, replace or upgrade equipment and achieve Cyber Essentials certification. The evaluation also demonstrated positive outcomes from staff training across all six key digital skill areas, enhancing knowledge in cybersecurity, data management and productivity.

The Tech Secure model has proven effective not only in mitigating immediate digital risks facing community and voluntary organisations but also in laying the groundwork for long-term resilience. It offers a model that charities can adopt to strengthen their digital infrastructure through structured device management, better informed staff

and improved digital governance. With ongoing support available via a low-cost monthly subscription, organisations are better equipped to maintain secure and efficient operations in an increasingly digital landscape. Based on this evaluation, Tech Secure presents a replicable model with the potential to strengthen the sector's digital skills and knowledge, reduce regional cybersecurity risks and enable organisations to operate safely and confidently while continuing to support the people and communities they serve.

Part 1: Background

Introduction

The Bytes Project established Bytes Digital Innovation Ltd as a subsidiary to support the improvement of the digital infrastructure of the community and voluntary sector. Bytes Digital Innovation Ltd has a unique focus on charities supporting children and young people. During 2025, The Bytes Project, through its subsidiary Bytes Digital Innovation Ltd, secured funding from Innovate UK to develop the Tech Secure project which piloted support for four community and voluntary organisations to develop a solid and innovative cyber security ecosystem. Developed in partnership with Kero Business Solutions and Reconome, the project involved assessing current digital infrastructure, upgrading equipment and providing training to build staff knowledge and confidence in using digital tools to support their work with children and young people.

Stats & Stories was commissioned to evaluate the effectiveness and impact of the Tech Secure pilot in strengthening digital capacity among community and voluntary organisations. The evaluation combined data from the initial needs assessment conducted by Bytes Digital Innovation Ltd with pre- and post-training surveys completed by staff, alongside three qualitative interviews with representatives from participating organisations. This mixed-methods approach provided insight into both measurable outcomes and participants' experiences of the support received.

Background

A recent scoping study commissioned by the Community Foundation, "A Digital Hub for the VCSE Sector in Northern Ireland"[1] in 2025, found that digital support across the community and voluntary sector remains highly uneven, with considerable variation in provision and access. Survey results indicated that 41% (n =139) of organisations reported having no IT support at all. While larger organisations often have dedicated IT resources, smaller charities face a range of barriers to accessing the support they need, particularly in terms of cost and limited in-house expertise.

[1] Community Foundation for Northern Ireland (2025) A *Digital Hub for the VSCE Sector: Scoping Study*. Available here

This corroborates findings from the 'Wired Up?'[2] report in 2022, which explored the significant digital challenges facing the community and voluntary sector in Northern Ireland. The report identified:

- Wide variation in digital skills across the sector, with many organisations lacking the capacity to operate confidently in a digital environment.
- Limited access to training opportunities to build digital competence within voluntary and community organisations.
- A lack of dedicated digital support services to help organisations establish and maintain effective digital infrastructure.
- Little core funding available for digital development, leaving organisations to absorb high and ongoing digital infrastructure costs with little support.

As a result of these challenges, many community and voluntary organisations lack the resources to ensure their staff are upskilled, technology is up-to-date or their systems are adequately protected. This has the potential to leave some organisations exposed to serious digital risks. In reality, risks look like staff using outdated or unmanaged computers, expired antivirus software and weak or shared passwords. Without the proper user access and management controls in place, sensitive data could be accessed or misused more easily. This has the potential to breach UK General Data Protection Regulation (GDPR) which may carry legal, financial and reputational consequences. To reduce these risks, organisations need basic digital infrastructure in place, such as device management, up-to-date security software and clear access controls, to help prevent data breaches and cyber-attacks.

The Tech Secure project was developed to address these gaps by piloting an affordable and scalable solution tailored to community and voluntary youth organisations. This pilot tests a model where organisations pay a small monthly fee to access support in assessing their digital infrastructure, renting devices, staff training and receiving ongoing IT support.

[2] Kernaghan, D. and Dallas, S. (2022) *Wired Up? Exploring the current levels of digital skills and inclusion in the Voluntary, Community and Social Enterprise Sector in Northern Ireland.* Available here

What is Tech Secure?

The Tech Secure pilot is a strategic initiative led by Bytes Digital Innovation Ltd, a social enterprise established by The Bytes Project to enhance the digital infrastructure of the community and voluntary sector.

The Tech Secure project was designed to support voluntary and community organisations working with children and young people in Northern Ireland to enhance their digital infrastructure, improve cybersecurity resilience and upskill staff. Specifically, Tech Secure aims to:

- Build digital capacity across the sector through tailored training and ongoing support;
- Enhance cyber security readiness and reduce risk exposure for voluntary organisations working with children and young people;
- Promote digital inclusion by ensuring access to up-to-date, secure devices and support;
- Support sustainability through a circular economy model and affordable, long-term service delivery.

To achieve these aims, Bytes Digital Innovation Ltd has established collaborations with two key partners:

Kero Business Solutions: Kero supplied Microsoft 365 tenancies and managed IT support

Reconome: Reconome provided refurbished laptops to support digital inclusion efforts as part of the circular economy.

The Tech Secure Approach

The approach taken by Tech Secure ensured that participating organisations had both: (i) the technical infrastructure; and (ii) the skills base needed for long-term digital resilience and secure service delivery. The table below outlines the delivery approach taken through the project, highlighting the core activities, the responsible partners and the specific outputs delivered. This structured, partnership-based model

ensured that each element of the programme was coordinated and led by organisations with relevant expertise.

Table 1: The Tech Secure Approach

Core Activity	Responsible Partners	Delivery
Needs Assessment of Digital Skills and Cybersecurity Awareness	Bytes Digital Innovation Ltd in conjunction with Kero Business Solutions	Conduct surveys/interviews to evaluate staff's current digital competencies and awareness of cybersecurity risks
Needs Assessment of Cybersecurity Infrastructure	Bytes Digital Innovation Ltd in conjunction with Kero Business Solutions	Audit current devices, software, and practices to identify gaps and vulnerabilities
Device Replacement	Reconome	Replace devices over two years old with refurbished laptops
Establish Microsoft Tenancies and Configure Devices	Kero Business Solutions	Set up Microsoft environments under charity licences
Remote IT Support	Kero Business Solutions	Provide ongoing technical support and maintenance for devices
Cyber Essentials Certification for Devices	Kero Bytes Digital Innovation Ltd	Ensure cybersecurity compliance across devices
Cyber Security Training	Bytes Digital Innovation Ltd	Deliver training on Cyber Hygiene Practices and tailored training based on initial assessments to strengthen digital skills and cyber resilience

Each participating organisation's journey through the programme followed a clear three-stage process as outlined below.

Stage 1: Cyber Infrastructure Needs Assessment

Bytes Digital Innovation Ltd, in partnership with Kero Business Solutions, carried out a detailed assessment to understand the specific digital needs of each participating organisation. This was conducted in two parts:

- **A technical audit to evaluate existing IT infrastructure**: This included the condition of devices, software in use and the presence (or absence) of core security features like firewalls, antivirus software and secure cloud storage.
- **Assessment of staff's digital skills:** Through pre-surveys and structured interviews to gauge the current level of staff confidence in using digital tools and understanding basic cybersecurity practices.

This initial needs assessment provided a baseline from which a tailored support plan was developed to meet the needs of each participating organisation.

Stage 2: Technical Implementation

Once technical and training needs were clearly identified, the project moved into its implementation phase. Outdated software was updated where possible. Where updates were not sufficient, devices were replaced with high-quality refurbished laptops, sourced through Reconome, supporting a circular economy and environmental sustainability.

Bytes Digital Innovation Ltd, in partnership with Kero Business Solutions, set up Microsoft 365 Business Premium tenancies for each organisation, taking advantage of the free charity licence scheme. Key cybersecurity measures were rolled out, including multi-factor authentication (MFA), endpoint protection and automated patch management which were all centrally managed and monitored to ensure consistent protection across all users. By the end of this stage, organisations were operating with a secure, standardised IT setup that allowed staff to collaborate and work more efficiently using cloud-based tools.

Stage 3: Staff Training and Capacity Building

Once the technical systems were in place, attention turned to building the knowledge and capacity of staff. The training provided by the Tech Secure project covered six key elements:

1. **Cybersecurity and Data Protection:** Training focused on Cyber Essentials compliance, including phishing awareness, secure data handling, password management and general cybersecurity best practices.

2. **Digital Communication and Collaboration:** Skills to confidently use collaboration tools like Outlook, Microsoft Teams and Zoom for effective internal and external communication.
3. **Data and Information Management:** Training on using SharePoint for document management and workflows, understanding cloud-based systems, and applying UK General Data Protection Regulation (GDPR) principles.
4. **Software and Digital Tools:** Practical training in Microsoft Word, Excel and PowerPoint for everyday tasks, alongside an introduction to Customer Relationship Management (CRM) software.
5. **Accessing IT Support:** Guidance on basic troubleshooting for devices, Wi-Fi and connectivity issues and how to access technical support when needed.
6. **AI Awareness:** Introduction to AI-powered tools like Microsoft Copilot, ChatGPT and AI scheduling assistants to support a range of tasks, with an emphasis on responsible and ethical usage in the workplace.

Section 2: Results

All four participating organisations from the community and voluntary sector worked with children and young people. Each organisation received a standardised framework which included:

- **Microsoft 365 Business Premium tenancy** with full Azure AD integration;
- **User accounts** configured with mandatory MFA and conditional access policies;
- **Devices upgraded** to Windows 11 Pro with complete Intune management
- **Azure AD Identity Management**: Migrated from local accounts to cloud-based identity system;
- **Exchange Online Configuration**: Professional email system with 50GB mailboxes per user;
- **SharePoint Online Deployment**: Centralised document management with version control;
- **Microsoft Teams Integration**: Secure communication and collaboration platform;
- **Complete security stack** including Microsoft Defender for Business, BitLocker encryption, and conditional access policies;
- **Security implementation** including Microsoft Defender for Business, BitLocker encryption, and automated threat response;
- **Managed services framework** with 24/7 monitoring, automated patching through Microsoft Endpoint Manager, and technical support;
- **Complete training programme** including cybersecurity awareness, Teams/SharePoint productivity, and responsible AI implementation;
- **Cyber Essentials certification** achieved using the standardised training and implementation approach.

The technical implementations differed only in scale based on their user and device counts as displayed in Table 2. Please note, the organisations who participated in the Tech Secure pilot have been anonymised to protect their privacy and confidentiality.

Table 2: Technical Implementation Summary by Organisation

Organisation	Technical Implementation
Organisation 1 Belfast	• **5 user accounts** configured with mandatory MFA using Microsoft Authenticator • **5 devices upgraded** to Windows 11 Pro with full Microsoft Intune management
Organisation 2 Enniskillen	• **6 user accounts** configured with mandatory MFA using Microsoft Authenticator • **6 devices upgraded** to Windows 11 Pro with full Microsoft Intune management
Organisation 3 Ballymoney/Derry	• **14 user accounts** (split between Ballymoney and Derry sites) with mandatory MFA implementation • **14 devices total** upgraded to Windows 11 Pro with centralised Intune management
Organisation 4 Belfast	• **5 user accounts** configured with mandatory MFA and conditional access policies • **5 devices upgraded** to Windows 11 Pro with complete Intune management

Stage 1: Digital Infrastructure Needs Assessment Results

Bytes Digital Innovation Ltd conducted a comprehensive needs assessment to understand the organisation's digital skills and cybersecurity awareness. This involved surveys and interviews with staff to evaluate their current competencies and awareness of cybersecurity risks. In parallel, the organisation's cybersecurity infrastructure was audited, reviewing devices, software and existing practices to identify gaps and weaknesses.

The needs assessment revealed several critical security vulnerabilities across the participating organisations' IT infrastructure. Key issues included:

- the use of a consumer-grade router with default credentials which exposed the network to easy exploitation from hackers;
- multiple open ports accessible on the public IP, increasing the risk of remote attacks;

- the absence of network segmentation which allows potential attackers to move freely across the network if they gained initial access.

On the endpoint side, significant gaps were identified. Several staff devices were unmanaged, running mixed Windows versions with local accounts and antivirus protection was either expired or non-existent. The lack of a patch management system meant known vulnerabilities remained unaddressed. In addition, unrestricted local administrator rights and shared computer profiles without password requirements created opportunities for privilege escalation and unauthorised access. Organisations also lacked centralised identity management and access controls which presented a major data security risk. Collectively, these weaknesses underscored the urgent need for improved network security, robust endpoint protection, stronger access controls and better management of devices and credentials to reduce exposure to cyber threats.

In order to remedy these critical issues uncovered by Stage 1, the Tech Secure project implemented a standardised technical stack across all participating organisations. This included successfully establishing Microsoft 365 tenancies, deploying managed endpoint security and implementing centralised user management with multi-factor authentication across all participating organisations. This was key to ensuring consistency and enabling efficient management. The technical implementation aspect of the project achieved:

- 4 organisational Microsoft 365 Business Premium tenancies established and configured;
- 26 devices total upgraded to Windows 11 Pro with complete managed endpoint protection;
- 32 user accounts total deployed across all organisations with 100% Multi Factor Identification (MFA) implementation;
- Standardised security framework deployed across all participating organisations;
- 24/7 monitoring and automated patch management implemented uniformly.

Case Study 1: A Small Charity's Digital Transformation

The office manager of a small mental health charity, with three staff and around 20 volunteers, recalls the moment they realised action was urgently needed. "We knew we had more work to do but when my emails got hacked and false invoices were being sent to my contacts, this highlighted our weakness and we knew we needed to get support to make our systems and processes more secure."

With support from Kero and Bytes, and access to funding, the organisation began the process of strengthening their digital infrastructure and working towards Cyber Essentials certification.

One of the first changes was upgrading from Windows 10 to Windows 11, and moving from Microsoft Office Home to a full Microsoft 365 tenancy setup. The organisation wiped everything from their PCs and removed the office hard drive. File management was moved to cloud-based SharePoint: "Before this, SharePoint was like an alien to us."

Another key change was the introduction of two-factor authentication in the office. "Now we use a phone to authorise access which added another layer of security." The organisation also updated its policies for how information is shared and introduced unique logins for all users.

While prioritising improved security, the team wanted to ensure they could still provide access to a computer for young people needing to work on CVs or job applications. "They appreciate and need this so we have one PC not connected to the network which guests are able to use without compromising our system."

The office manager reflects that: "It is a challenge to change the culture, there has been a steep learning curve but this project has given us the building blocks to move in the right direction." He notes that having external support helped

Stage 3: Tech Secure Staff Training Results

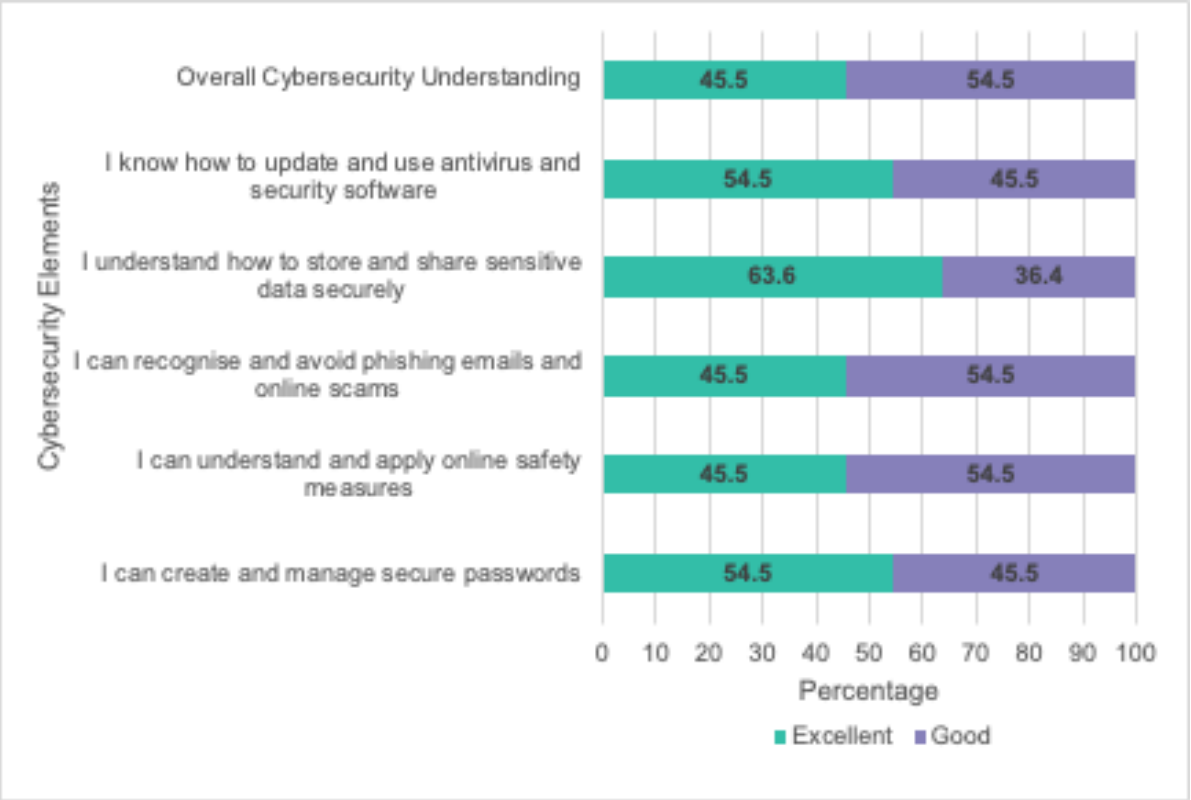
The evaluation methodology for the staff training element of the project followed a pre/post approach. Staff (n = 19) completed a pre-training survey to self-assess their skills across six key digital areas including cybersecurity and GDPR compliance, digital communication, data management, practical software skills, accessing IT support and an introduction to AI tools. After training, a subset (n = 11) completed a post-training survey using the same criteria. Three organisations also took part in interviews to develop case studies exploring their in-depth experience of the project. The results in the following section highlight the areas of greatest need before training and the improvements in staff knowledge and confidence afterwards.

Cybersecurity and Data Protection

Cybersecurity was the area where over one third of staff (36.9%) initially rated their abilities as fair or poor. While the majority of participants rated their ability to create and manage secure passwords and understanding and applying online safety measures as excellent or good (84.2%), staff's confidence in using antivirus and security software was relatively low, with 31.7% rating their skills as fair, poor and very poor.

As displayed in Figure 1 after training all participants rated their cybersecurity skills as excellent or good indicating the positive impact of the training on participants' general confidence and awareness around cybersecurity.

Figure 1: Participants' Self-Rating of Cybersecurity Skills After Tech Secure Training



N = 11

Case Study 2: How Cyber Essentials Transformed a Youth Charity's Digital Security

This Youth Engagement Charity is a small organisation working with young people in schools and youth centres, supported by a team of two full-time and two part-time staff. As the organisation looked to modernise its practices, a key concern was how to securely collect and store data while transitioning away from paper-based systems. It was also important that young people and parents could trust that their information was being handled safely. Prior to taking part in the Tech Secure programme, IT support was minimal and mostly reactive, only available when something broke.

Achieving Cyber Essentials certification became a priority when it was set as a requirement by the charity's core funder. With the help of Kero, the process became manageable. For the manager, the ability to access dedicated IT support meant they could stay focused on their core responsibilities: "I literally contact Kero and they can take over. That lets me do my job more effectively." The training delivered through the programme also improved staff awareness of cybersecurity, especially among colleagues who were not particularly tech-savvy.

The impact of certification has been significant. It was vital in securing core funding and has given the organisation confidence that it now has a certified, secure IT system in place. As the manager explained, "As a small charity I would definitely say this is important to have. We are in the digital age now." For this organisation, Cyber Essentials certification has not only improved digital resilience, it has also helped to build credibility and sustainability in a challenging funding environment.

Digital Communication and Collaboration

This aspect of training focused on equipping participants with practical skills to communicate and collaborate effectively using a range of digital tools. Topics covered included:

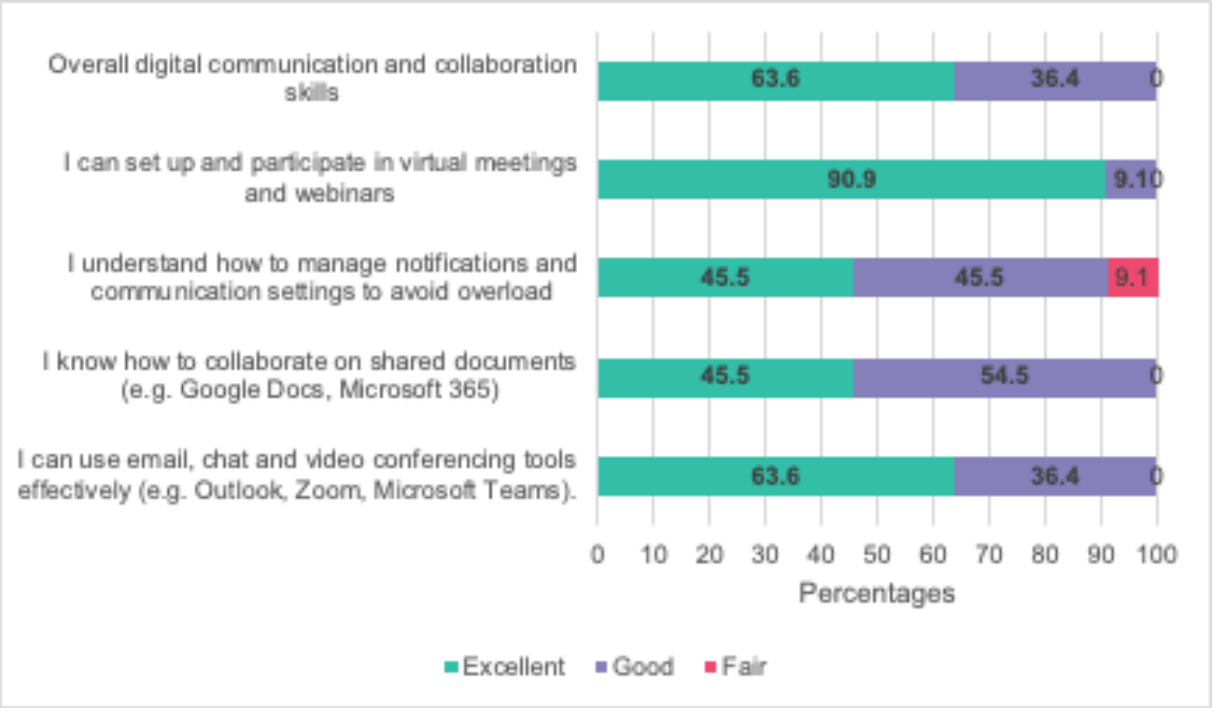
- using email, chat and video conferencing platforms such as Outlook, Teams and Zoom;
- collaborating on shared documents via Google Docs and Microsoft 365;
- setting up and managing virtual meetings and webinars; and
- managing notifications and communication settings to reduce overload and improve digital wellbeing.

Following the training, participants reported clear improvements across all areas. Confidence in setting up and participating in virtual meetings and webinars rose significantly from 78.9% rating themselves as excellent or good before training to 100% after, with 90.9% selecting excellent.

Skills in collaborating on shared documents also strengthened, with all participants post-training rating themselves at least good, compared to 15.8% pre-training who rated their skills lower. One of the most marked improvements came in managing notifications and communication settings. Before training, only 68.4% felt confident in this area which increased to 91.0% post-training.

Overall digital communication and collaboration skills improved, with 100% of participants post-training rating themselves excellent or good, up from 84.2% pre-training as shown in Figure 2.

Figure 2: Participants' Self-Rating of Digital Communication and Collaboration Skills After Tech Secure Training



N = 11

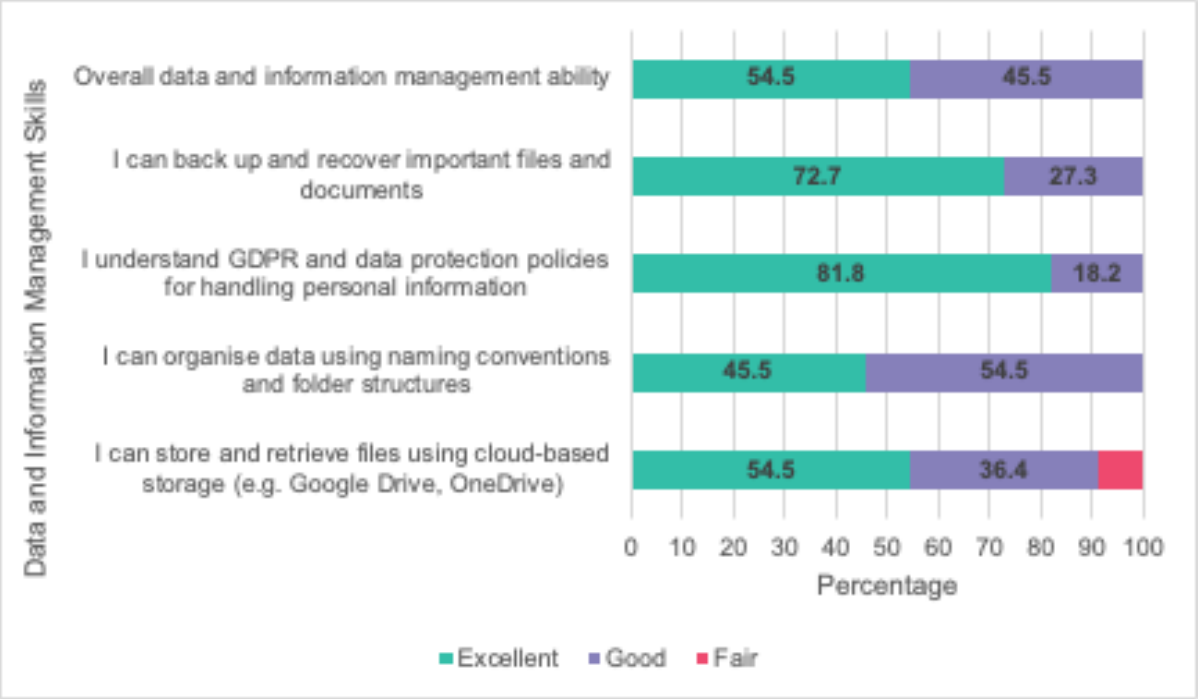
Data and Information Management

Some participants indicated significant gaps in knowledge around data and information management tasks. The greatest need for improvement was in backing up and recovering important files as over one third of participants rated (36.9%) their ability as fair or poor. Similarly, understanding of GDPR and data protection showed some gaps, with over 26.3% of participants rating their knowledge as fair or poor.

Following the training, confidence in both areas increased significantly. All participants rated their understanding of GDPR and data protection as excellent or good, and all felt confident in backing up and recovering files. Improvements were also seen in organising data using naming conventions and folder structures with 100% rating themselves as excellent or good post-training. Use of cloud-based storage tools, such as Google Drive and OneDrive, also improved. Overall,

participants demonstrated stronger and more consistent skills across all areas of data and information management.

Figure 3: Participants' Self-Rating of Data and Information Management Skills After Tech Secure Training



N = 11

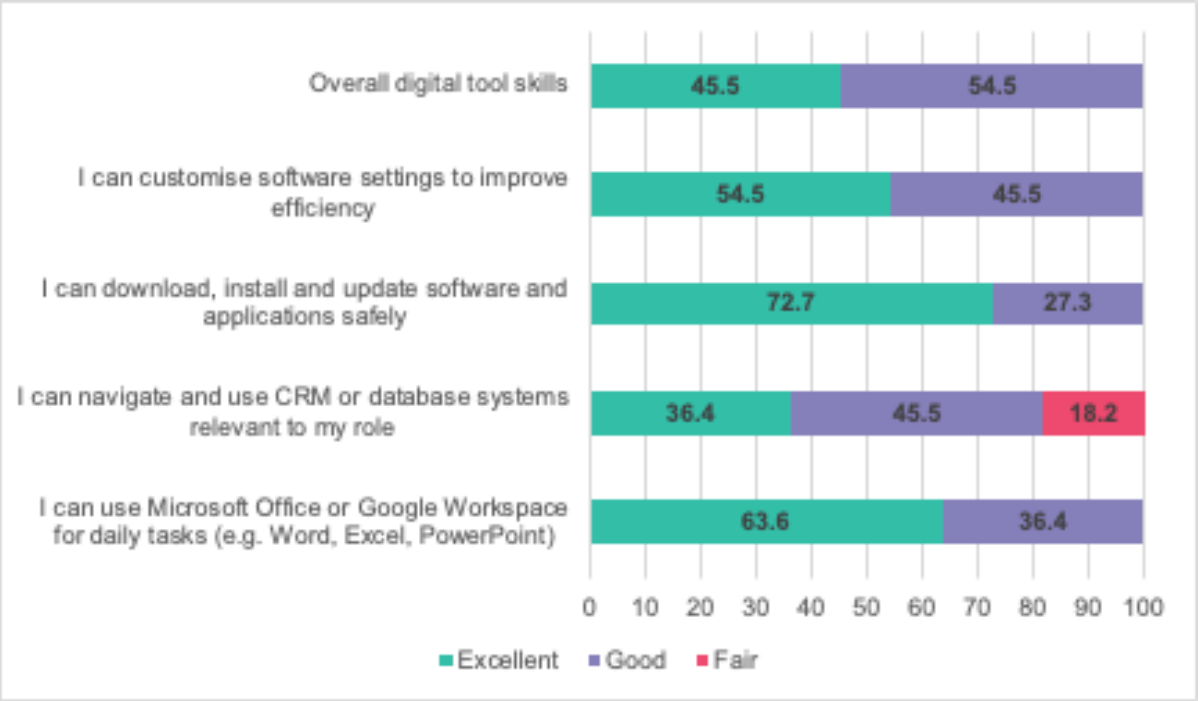
Software and Digital Tools

Most participants indicated they were generally confident in using basic digital tools, with 68.4% rating their overall digital skills as excellent or good. However, a sizeable proportion of users (31.6%) rated their digital skills as fair or poor before the training.

Confidence was strongest in using Microsoft Office or Google Workspace, with 94.7% rating themselves excellent or good before the training. In contrast, customising software settings to improve efficiency presents the highest level of need, with 36.9% of staff rating their ability as fair or poor. Similarly, 26.3% rated their ability to navigate CRM (customer relationship management) or database systems as fair or poor.

In addition, over a quarter of participants (26.4%) rated their ability to download, install and update software safely as fair or poor before the training. As shown in Figure 4, all participants rated their skills as excellent or good, except for 18.2% who still rated their CRM/database skills as fair.

Figure 4: Participants' Self- Rating of Digital Tools After Tech Secure Training



N = 11

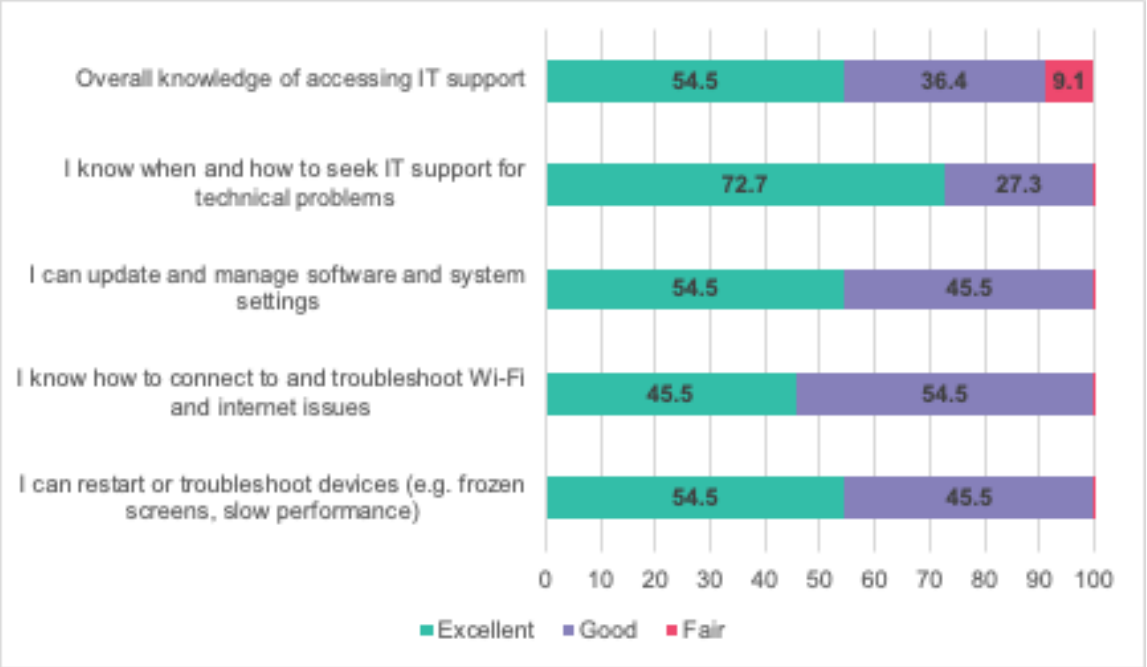
IT Troubleshooting and Support

Before the training, the majority of participants (68.8%) rated their overall knowledge of accessing IT support as excellent or good with 31.3% indicating their knowledge as fair or poor.

While most staff members felt they could deal with basic connectivity issues such as knowing when and how to seek IT support (83.3%) and troubleshooting Wi-Fi or internet problems (77.8%), confidence declined when it came to managing software and system settings with only 66.6% felt their skills to be excellent or good, while 33.4% rated themselves as fair or poor.

Results after training show that all participants rated their IT trouble shooting and support awareness across each specific area as either excellent or good, although one person considered their overall knowledge as fair (9.1%) after training.

Figure 5: Participants' Knowledge of IT Support After Tech Secure Training



N = 11

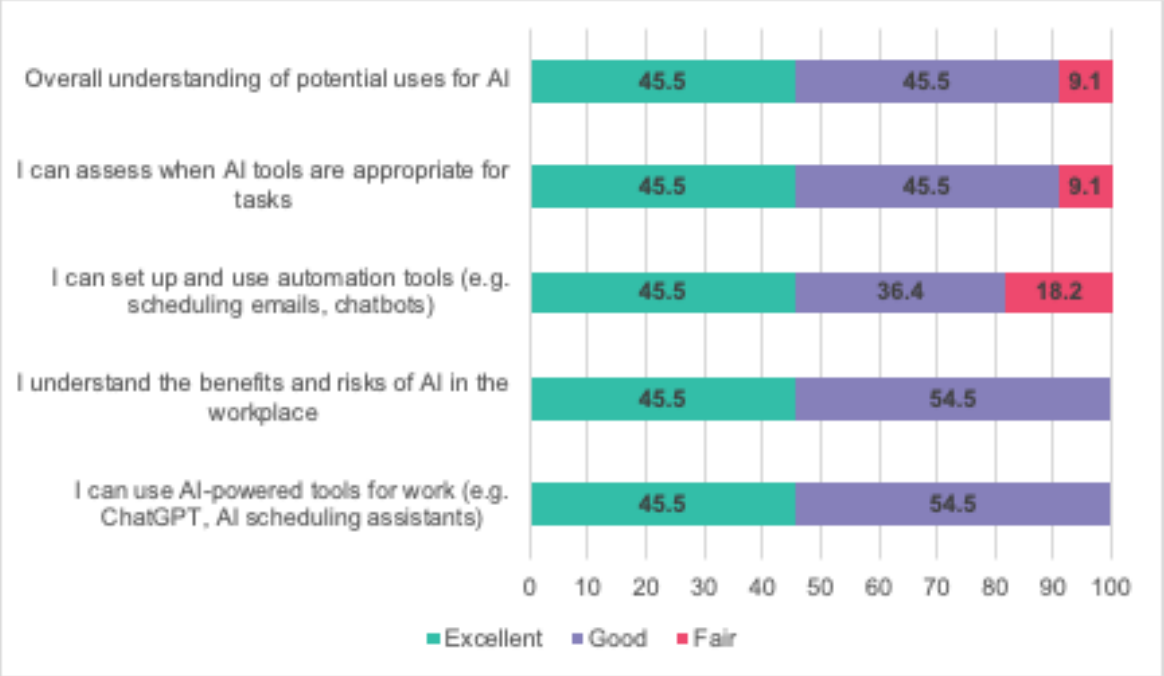
AI Awareness

Before the training, participants demonstrated a reasonable level of awareness of AI tools and understanding of their benefits and risks. Most rated themselves excellent or good in using AI-powered tools (88.8%) and understanding AI-related workplace implications (83.3%). However, the training also helped identify key areas of need. Confidence was notably lower in:

- Setting up and using automation tools: 44.5% rated themselves fair or poor
- Overall understanding of AI's potential uses: 33.3% rated themselves fair
- Assessing when AI tools are appropriate: 22.3% rated themselves fair or poor

These findings highlighted the importance of building practical, hands-on skills alongside conceptual understanding. The training addressed these gaps effectively, with the majority of participants rating themselves excellent or good in all areas post-training.

Figure 6: Participants' Awareness of AI After Tech Secure Training



N = 11

Case Study 3: How One Youth Work Charity Benefited from AI

Before engaging with the Tech Secure project, the manager of a youth-focused charity described their organisation as cautious when it came to digital transformation. The hesitation was rooted in fear of the unknown, concerns about GDPR and data protection, and a general lack of time to explore new approaches. Innovation to improve productivity often felt out of reach.

This changed when they joined the Tech Secure pilot. Through tailored support, the charity received refurbished, secure laptops via Reconome, Microsoft tenancies and managed IT support from Kero Business Solutions. Staff also participated in digital skills training delivered by Bytes Digital Innovation Ltd. An initial digital skills and cybersecurity assessment helped the organisation identify specific gaps and track progress.

One of the most notable changes since engaging with Tech Secure project has been the organisation's use of AI. With new confidence and infrastructure in place, the team began to explore how Microsoft Copilot and ChatGPT could support them in their work.

A key breakthrough came in their youth programming. Using feedback from young people and support from ChatGPT, staff co-designed session plans that not only met the needs of their participants but also aligned with funder targets. AI offered creative suggestions for games, icebreakers and even helped name projects which unexpectedly increased buy-in from young people.

The team also discovered that AI could ease the burden of fundraising. ChatGPT was used to draft funding applications which improved quality and saved time. When it came to monitoring and reporting, staff used AI to analyse anonymised data from pre- and post-programme surveys. This transformed raw feedback into clear results. Although they acknowledged the importance of reviewing and verifying AI-generated content, the use of AI significantly saved time and improved the clarity of their reports.

Reflecting on the impact, the manager said that the Tech Secure training did not just provide new tools it also encouraged staff to be more open, more curious and more confident about exploring technology, especially AI, as a way to support their work and strengthen outcomes for young people.

The Tech Secure training led to positive change across all key digital competency areas. The most significant improvement was observed in Cybersecurity and Data Protection which increased markedly from 63.1% to 100%, indicating a substantial rise in awareness of safe digital practices. There were also notable gains in Data and Information Management Skills and Software and Digital Tools Skills, both improving from 68.4% to 100%. This demonstrates a strong enhancement in managing digital information and utilising essential software effectively.

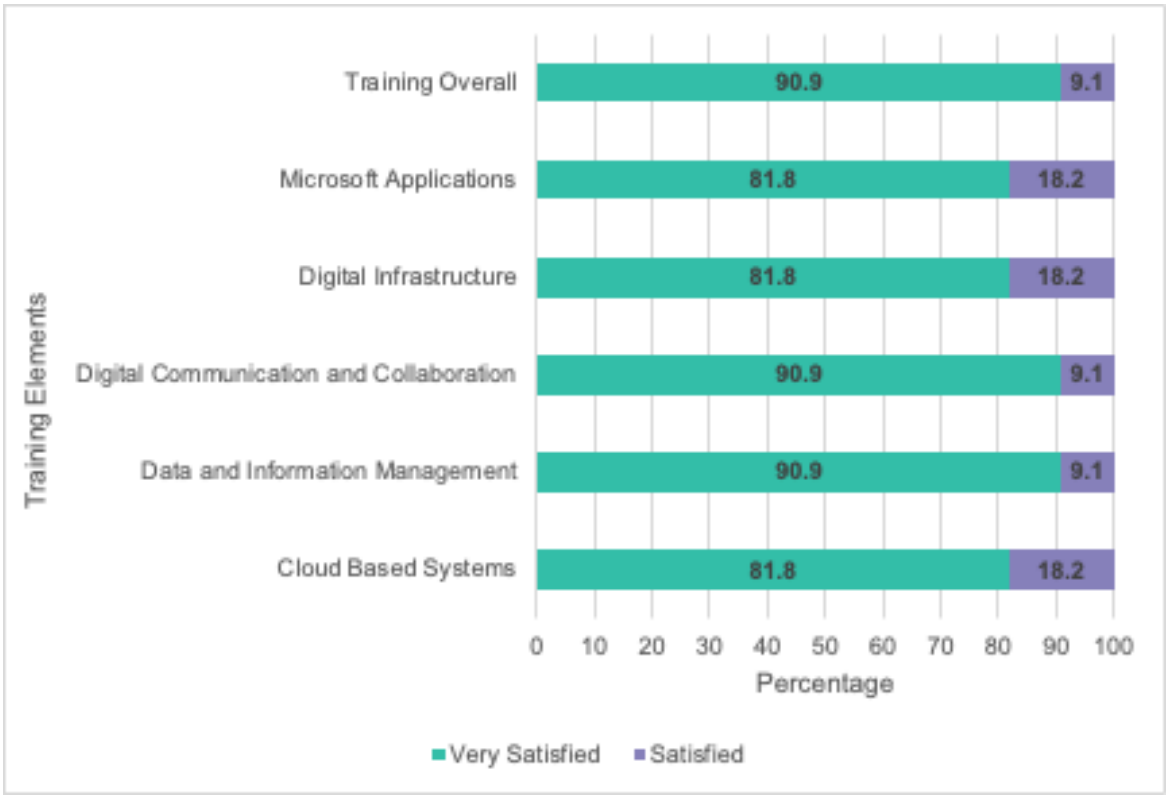
AI Awareness also showed a considerable increase, rising from 66.7% to 91.0%, which reflects a meaningful improvement in understanding and confidence in emerging technologies. Awareness of Accessing IT Support was more modest, improving from 68.8% to 90.9% as shown in Table 3. Every area experienced positive growth which highlights the broad effectiveness of the Tech Secure training in strengthening staff's digital skills and capacity.

Table 3: Overall Impact of Tech Secure Training on Staff's Digital Skills

Digital Skills	Pre Training % Excellent/ Good (n = 19)	Post Training % Excellent/Good (n = 11)
Cybersecurity and Data Protection Understanding	63.1	100
Digital Communication and Collaboration Skills	84.2	100
Data and Information Management Skills	68.4	100
Software and Digital Tools Skills	68.4	100
Awareness of Accessing IT Support	68.8	90.9
AI Awareness	66.7	91.0

Satisfaction with Training: The data indicates a high level of staff satisfaction with the training provided by Bytes Digital Innovation Ltd across all areas. The majority of participants rated each aspect as very satisfied as shown in Figure 7, with particularly strong responses for Data and Information Management and Digital Communication and Collaboration with 90.9% reporting being very satisfied.

Figure 7: Participants Satisfaction with Tech Secure Training



N = 11

All participants also rated the effectiveness of the overall training from Bytes Digital Innovation Ltd as very effective (81.8%) or effective (18.2%).

Conclusion

The evidence suggests that the Tech Secure project has significant potential to help community and voluntary organisations tackle persistent challenges in establishing and managing their digital infrastructure. Common risks identified through the Tech Secure needs assessment process included absence of a managed IT infrastructure, vulnerability to hacking, lack of antivirus protection and use of inappropriate or outdated equipment and software. In addition, staff in participating organisations required training on data management, cybersecurity and troubleshooting to safeguard sensitive information and maintain system integrity. Staff also needed support to develop their own skills and knowledge on how to make better use of digital tools and boost productivity through AI.

The pilot directly addressed these challenges by supporting organisations to implement managed IT systems, replace or upgrade equipment and achieve Cyber Essentials certification. The evaluation also demonstrated positive outcomes from staff training across all six key digital skill areas, enhancing knowledge in cybersecurity, data management and productivity.

The Tech Secure model has proven effective not only in mitigating immediate digital risks facing community and voluntary organisations but also in laying the groundwork for long-term resilience. It offers a model that charities can adopt to strengthen their digital infrastructure through structured device management, better informed staff and improved digital governance. With ongoing support available via a low-cost monthly subscription, organisations are better equipped to maintain secure and efficient operations in an increasingly digital landscape. Based on this evaluation, Tech Secure presents a replicable model with the potential to strengthen the sector's digital skills and knowledge, reduce regional cybersecurity risks and enable organisations to operate safely and confidently while continuing to support the people and communities they serve.