Department for Education

Cyber Check for schools

Welcome

Arati Patel-Mistry
Cyber Security Engagement Lead

George Martin
Security and Data Protection Advisor- SWGfL

Department for Education

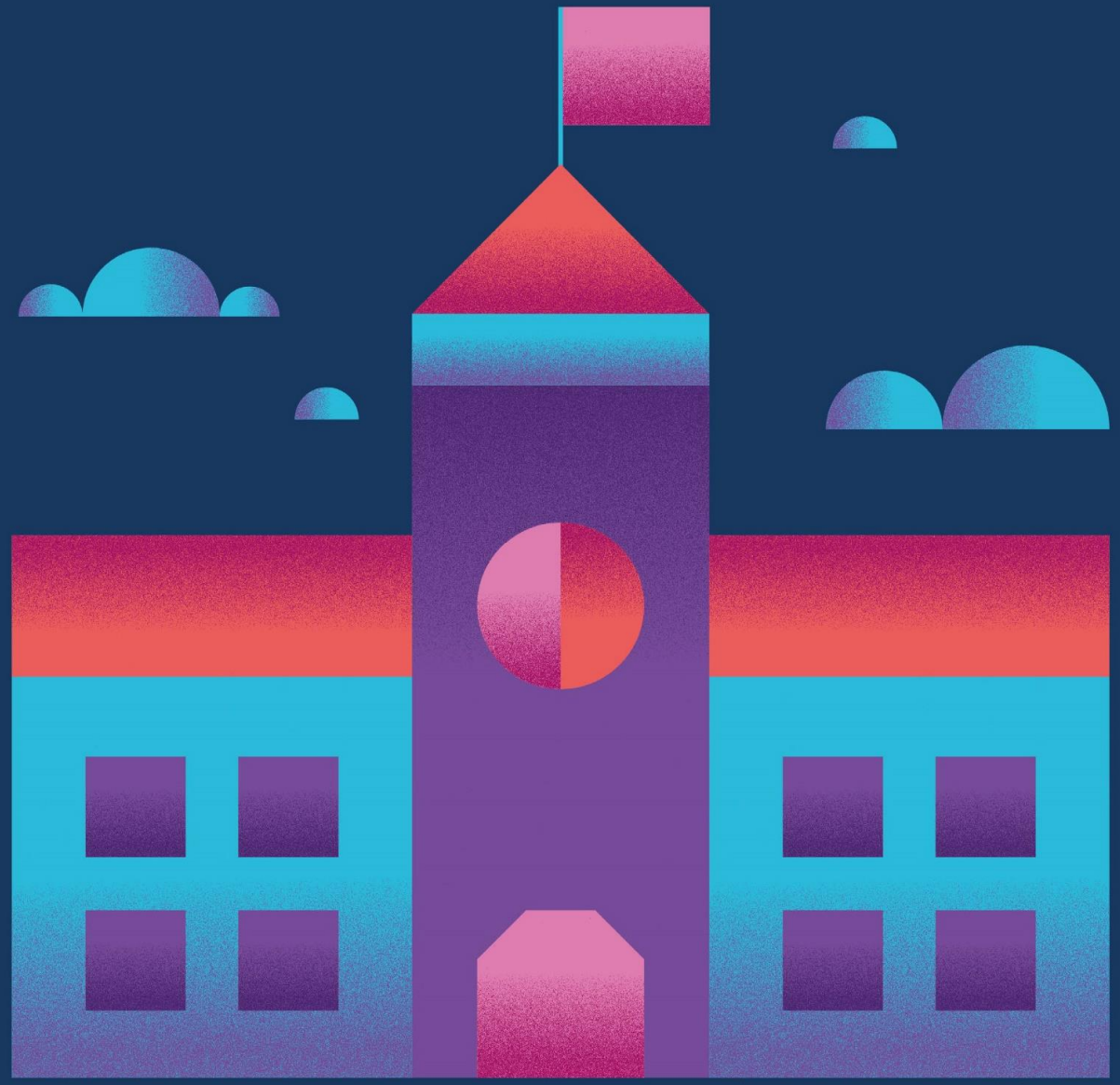
Today we will cover…

- DfE Cyber Security Standards
- Cyber threat in education
- ‘Cyber check for schools’ Cyber Secure – start guide
- Links to further support

Digital Data Technology

Digital and technology standards

June 2024



Department for Education

Why is it important to have safe and reliable tech?

- Increasing efficiency across school estate
- Improving accessibility and inclusion
- Improving cyber resilience and security
- Reducing the risk of online harms
- Supporting excellent teaching
- Contributing to improved workload efficiencies
- Contributing to improved student outcomes

Digital and technology standards

Connectivity

- Broadband Internet
- Wireless network
- Network switching
- Network cabling

Prevention of Harms

- Filtering and Monitoring
- Cyber Security

Efficiencies and Optimisation

- Leadership and Governance
- Laptops, desktops and tablets
- Digital accessibility
- Servers and storage
- Cloud solution

Who are the standards for?

Scan to access Digital and Technology Standards

Everyone involved in the planning and use of technology within schools and colleges, including:

- **Senior leadership teams**
- **IT staff**
- **Suppliers**
- **Technical advisers**
- **Teachers**
- **Governors**

What we've heard from schools so far...

"As a member of SLT with less technical experience I found them to be clear and incredibly useful they would help me to ask of others and answer questions around these aspects. These standards would drive improvement."

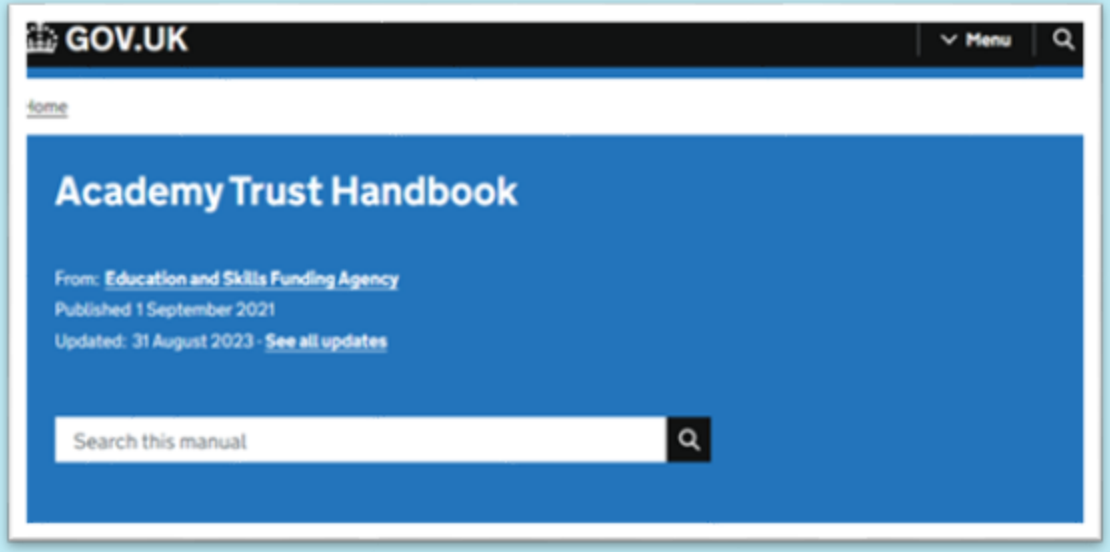
"These standards read well - they make you do something but without being scaremongering."

"It is a good starting point for educational establishments to refer to when looking at IT procurement, especially when dealing with salespeople."

Cyber Standards Refresh

The key changes are:

- More information for Senior Leaders
- The 12 standards have been condensed into 7
- Updated structure to fit the existing suite of standards



SCAN ME

→ To access Cyber Standards

What are the changes and why are they important?

New standard	This standard addresses elements of the existing standard titled:
Standard 1 – Conduct a cyber risk assessment annually and review every term	Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack’
Standard 2 – Create and implement a cyber awareness plan for students and staff	Train all staff with access to school IT networks in the basics of cyber security
Standard 3 – Secure digital technology and data with anti-malware and a firewall	Protect all devices on every network with a properly configured boundary or software firewall Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date You should use anti-malware software to protect all devices in the network, including cloud-based networks An administrator should check the security of all applications downloaded onto a network

What are the changes and why are they important?

New standard	This standard addresses elements of the existing standard titled:
Standard 4 – Control and secure user accounts and access privileges	Accounts should only have the access they require to perform their role and should be authenticated to access data and service You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication
Standard 5 – License digital technology and keep it up to date	All devices and software must be licensed for use and should be patched with the latest security updates
Standard 6 – Develop and implement a plan to backup your data and review this every year	You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be offsite
Standard 7 - Report cyber attacks	Serious cyber-attacks should be reported

Digital Data Technology

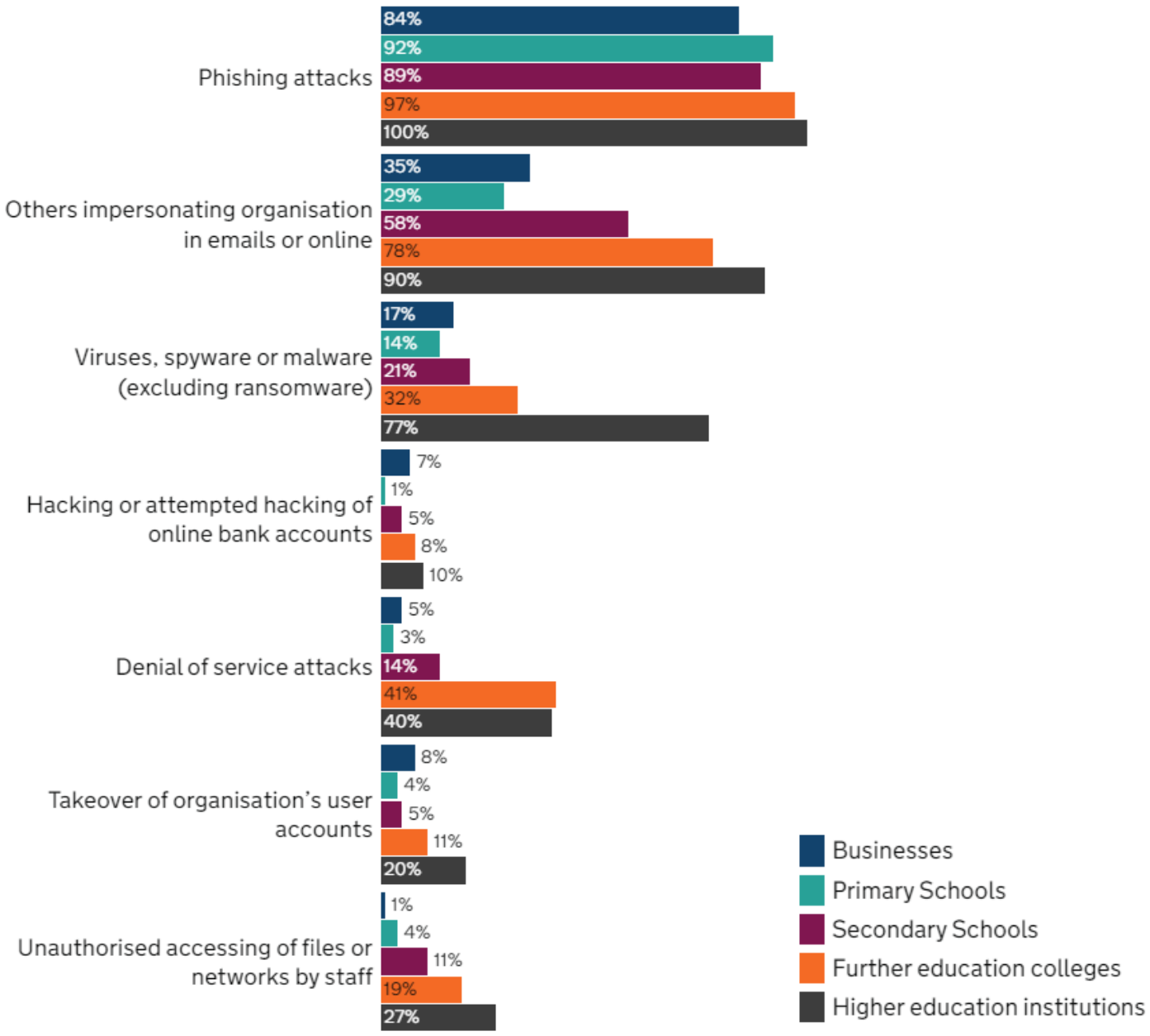
Cyber Threat in Schools

Department for Education

CYBER THREAT

52% of primary, 71% of secondary schools and 86% of further education colleges identified cyber breaches or attacks 2023 – 2024*

**DSIT Cyber Security Breaches Survey 2024*



ITPro. Business Cloud Hardware Infrastructure Security Software Technology Resou

15 schools in Nottinghamshire crippled by cyber attack

The Nova Education Trust is unable to access its IT systems to conduct remote lessons

by Bobby Hellard 4 Mar 2021

Schools across Nottinghamshire have had to shut down their IT networks after a central trust that manages their systems was hit by a cyber attack.

All 15 secondary schools that are part of the Nova Education Trust are currently unable to access emails or their websites, and are still unable to conduct lessons remotely.

- Hackers hold Newcastle University data to ransom
- Exams cancelled after hot thumbs in University cyber attack
- What is ransomware?

The trust has alerted the National Cyber Security Centre (NCSC) which is currently working with its central IT team to resolve the matter. The incident has also been reported to the Department of Education (DfE) and the Information Commissioner's Office (ICO).

The attack was first discovered on Wednesday morning, prompting the trust to shutdown every one of its systems as a

ISLE OF WIGHT SCHOOLS NEED DATA AFTER CYBER ATTACK

News Home | More from Isle of Wight News

Tuesday, August 24th, 2021 10:28am

By Oliver Dyer @oldyer

Parents of students at Isle of Wight schools hit by ransomware attacks are being asked to get in touch after vital data was lost.

As Isle of Wight Radio first reported, cyber attacks left school websites inaccessible and data 'frozen' earlier this month.

Staff at Medina and Carisbrooke College, as well as the Island VI Form, were affected, as were Barton Primary, Hunnyhill Primary and Lanesend Primary.

As such, affe

Fears as 'thousands' of cyber attacks launched against British schools and universities

SUBSCRIBE

IE NEWS FEATURES COMMENT WEBINARS PODCAST EVENT REPLAY DIRECTORY PROFILE LOGIN

Independent Education Today | For leaders of independent schools

The growing importance of cybersecurity in schools

Sponsored: iSAMS explores the most effective ways schools can protect themselves against cyber scammers

Contributor

In 2020, the UK's Department for Digital, Culture, Media and Sport conducted a Cyber Security Breaches Survey with a section focused specifically on the education sector. Its findings made for perturbing reading. The results of the survey showed that 41% of primary schools, 76% of secondary schools and 80% of further education institutions had identified at least one cyber-attack or security breach in the previous 12 months.

Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions – seen as low hanging fruit – that may be less well equipped to deal with a scam or hacking attempt. The fallout from a security breach can have devastating consequences for schools.

Previous attacks have resulted in significant financial losses, sensitive data on students, parents and staff being lost or published online and have even forced temporary school closures. With schools firmly in the crosshairs of cybercriminals, the importance of a secure digital infrastructure has never been greater.

One of the most effective ways to protect against cyber scammers is training staff to spot phishing attacks and malicious downloads, and implementing safety checks such as 2FA (two-factor authentication) for all school systems.

Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions

Cybercriminals can embed malware in email attachments, which if downloaded can spread through a school's network

Sign up for email upd all the latest support

fe news.co.uk

HOME PUBLISH SEARCH FEATURES VIDEO & PODCASTS SECT

93% increase in cyberattacks targeting the UK's education sector

by Check Point Research Published: 23 August 2021 Hits: 1255 Vote 5 Rate

As back-to-school begins, Check Point Research (@_CPResearch_) found the education sector to have the highest volume of cyber attacks for the month of July. Cyber criminals are seeking to capitalize on the short-notice shift back to remote learning driven by the Delta variant, by targeting people of schools, universities and research centers who log-in from home using their personal devices.

93% increase in cyberattacks targeting the UK's education sector

- Global education sector saw a 29% increase in cyber attacks, and an average of 1,739 attacks a week, in July, compared to first half of 2021
- Top 5 most attacked countries were India, Italy, Israel, Australia and Turkey
- UK/Ireland/Isle-of-Man region experienced a 142% increase in weekly cyber attacks targeting the education sector; East Asia region marked a 79% increase

Check Point Research (CPR) sees an increase in cyberattacks against the global education sector, as back-to-school season gets underway. During the month of July, the education sector experienced the highest volume of cyber attacks compared to other industry sectors that CPR tracks, with an average of 1,739 cyber attacks documented per organization each week, marking a 29% increase from the first half of 2021.

Mail

News Sport What's On Lifestyle Public Notices Advertise My Business Free Happy Ads

Man appears in court accused of cyber-attack on a Harborough school's computer network

The case has been referred to Leicester Crown Court

By Rod Williams

Threats Culture & Education Opinion Events Video teissTalk White Papers

Harris Federation suffers a ransomware attack, shuts down email and telephone systems

March 31, 2021

Education charity Harris Federation has become the fourth multi-academy trust to have suffered a ransomware attack since late February. The ransomware attack has forced the charity to shut down IT systems, and temprarily disable its email system and switchboard services.

The Harris Federation, which now runs fifty primary and secondary academies in London and Essex with more than 36,000 pupils enrolled, announced on Monday that it suffered a ransomware attack last Saturday that enabled hackers to access its IT systems and encrypt their contents. The charity is presently working with cyber security experts to investigate the attack and restore all affected systems.

In a press release, Harris Federation said that after discovering the ransomware attack, it disabled its email system used by more than 40,000 students, as well as its telephone systems and switchboard services as a precaution.

National Cyber Security Centre

ABOUT NCSC CRP REPORT AN INCIDENT CONTACT US

Home Information for... Advice & guidance Education & skills Products & services News, blogs, events...

Home • Alert: Further ransomware attacks on the UK education sector by cyber criminals

NEWS

Alert: Further ransomware attacks on the UK education sector by cyber criminals

The NCSC is responding to further ransomware attacks on the education sector by cyber criminals.

PUBLISHED
4 June 2021

NEWS TYPE
Alert

WRITTEN FOR
Large organisations
Small & medium sized organisations
Cyber security professionals
Public sector

Download / Print Article PDF

Share

Was this article helpful?
Yes No

IN THIS ALERT
1 Introduction

CONTEXT AND IMPACT – SO WHAT?

Ransom is the biggest threat facing the education sector

Over 143 incidents have been reported since August 2024

Schools are critically dependent on technology and online services

But it's a challenge to maintain IT infrastructure, processes & cyber awareness

… which means that schools become easier targets for cyber criminals

And so leaders want DfE support to help with their cyber and digital capabilities

- SERVICE
  e.g. school can't open, reception can't take calls
- PUPILS
  e.g. lost work, exams cancelled
- FINANCIAL
  e.g. lose a significant sum of money, staff/suppliers can't be paid
- LEGAL
  e.g. safeguarding data leaked
- REPUTATION
  Immeasurable

WHAT IS CYBER SECURE?

Free and anonymous self-assessment tool

Helps schools understand and improve their cyber resilience

Based on recognised standards

Iterative and will develop in line with industry best practice

SWGfL
Safe. Secure. Online

HOW DOES IT WORK?

https://CyberSecureCheckForSchools.uk

Grade your cybersecurity measures along 23 aspects

Anonymously compare performance with local/national averages

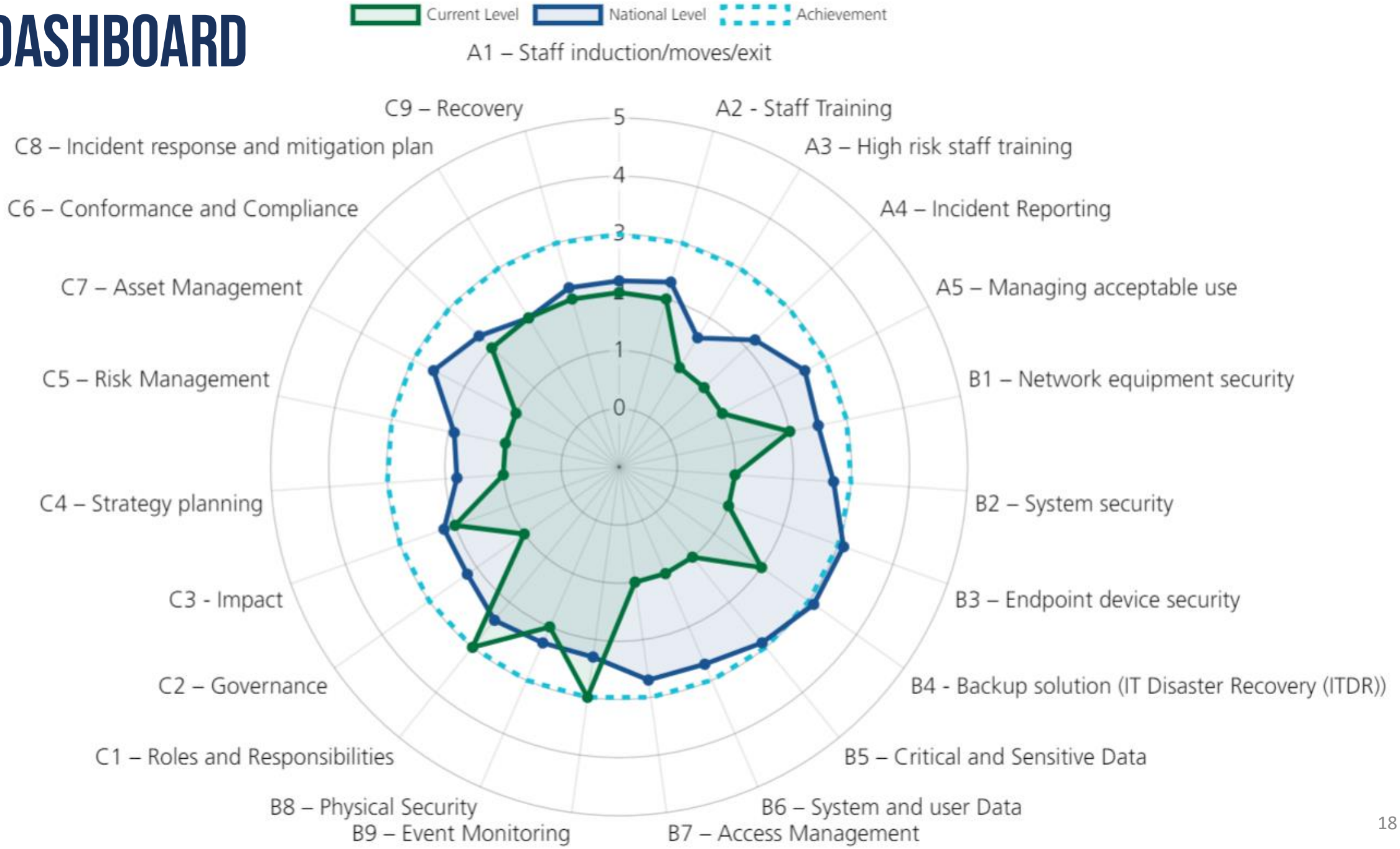
Report risk-based assessment to senior leadership to inform decision-making

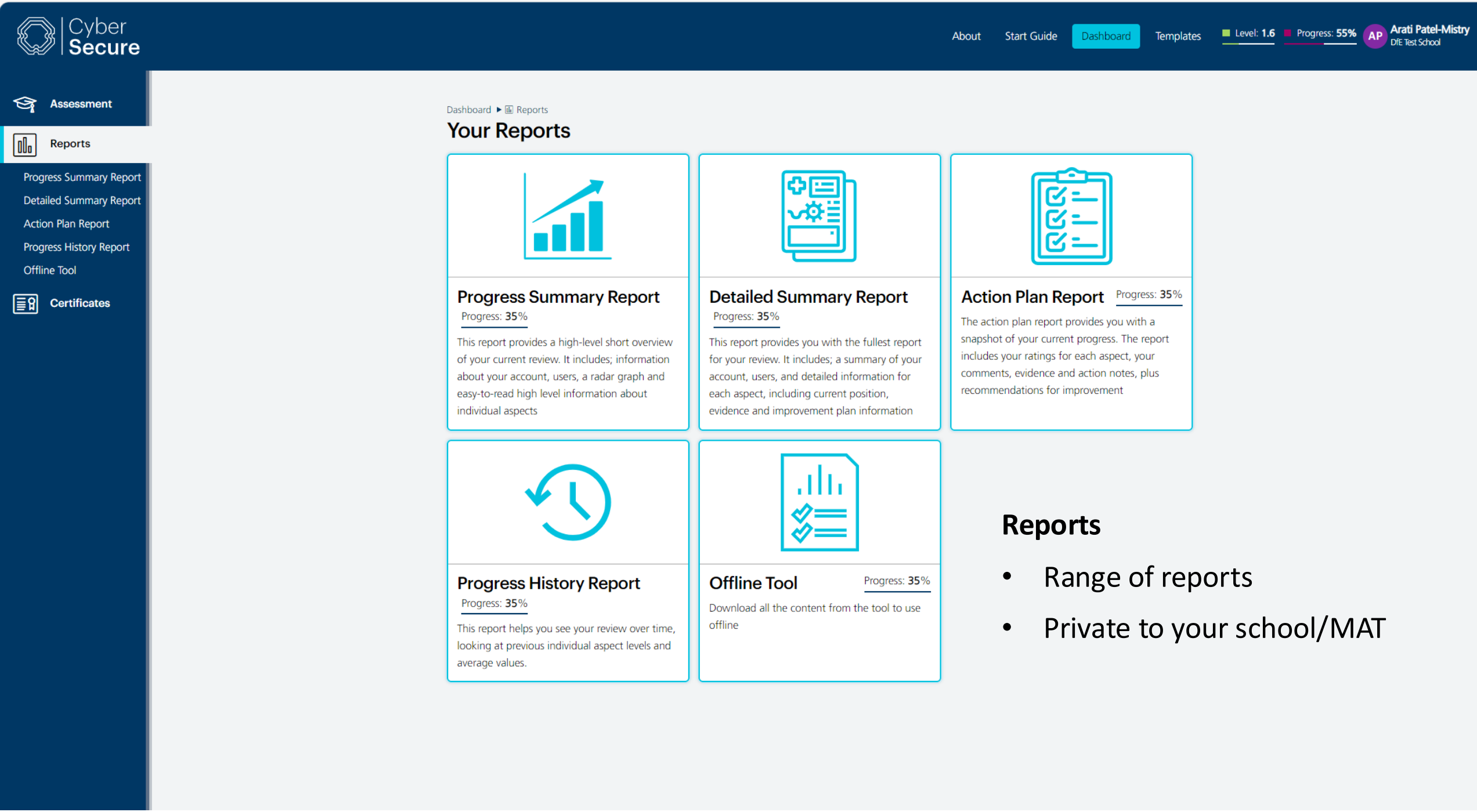
Includes guidance, templates and links to best practice resources

ASSESSMENT

A. People	e.g. staff induction
B. Systems	e.g. device security
C. Organisation	e.g. incident response

DASHBOARD


Current Level
National Level
Achievement
A1 – Staff induction/moves/exit
A2 - Staff Training
A3 – High risk staff training
A4 – Incident Reporting
A5 – Managing acceptable use
B1 – Network equipment security
B2 – System security
B3 – Endpoint device security
B4 - Backup solution (IT Disaster Recovery (ITDR))
B5 – Critical and Sensitive Data
B6 – System and user Data
B7 – Access Management
B9 – Event Monitoring
B8 – Physical Security
C1 – Roles and Responsibilities
C2 – Governance
C3 - Impact
C4 – Strategy planning
C5 – Risk Management
C7 – Asset Management
C6 – Conformance and Compliance
C8 – Incident response and mitigation plan
C9 – Recovery
5
4
3
2
1
0



Reports

- Range of reports
- Private to your school/MAT

Cyber Secure

About Start Guide Dashboard Templates Help Level: 1.7 Progress: 35% DS Demo School Demo School

Cyber Secure: Cyber Security Check up for Schools

Cyber Secure is free to use and helps you to review and improve your Cyber and Information Security in your school setting

Start Your Assessment

Building the foundations for cyber security

What is Cyber Secure?

Cyber Secure is a tool that allows schools to review and improve their cyber and information security policy and practice and self-assess their current provision. The tool is structured according to categories indicating the safety and security 'levels' establishments can achieve, with level 0 being the lowest and most basic, and level 5 the highest and most aspirational.

Why use it?

Cyber Secure is a powerful free tool designed by cyber and information security experts. Cyber Secure is designed to help achieve consistency in cyber security across educational establishments. It helps

Cyber Secure

83% of users highlighted improved knowledge about cyber security

Used by over 1000 schools

Department for Education

SWGfL
Safe, Secure, Online

Next steps

1. **Register at** https://CyberSecureCheckForSchools.uk

2. **Read the DfE Standards** DFE- Cyber security standards for schools and colleges

3. **Need further support?**
   About the Cyber Secure tool: cybersecure@swgfl.org.uk

   DfE Standards advice & guidance: sector.securityenquiries@education.gov.uk

4. **More resources and advice:**
   https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

5. **Need to report a cyber incident?**
   DfE: sector.incidentreporting@education.gov.uk
   Contact the relevant authorities: Police, Action Fraud
   Data breaches must be reported to the ICO

Q&A

Cyber Secure Frequently Asked Questions

https://cybersecurecheckforschools.uk/faqs/