Department for Education

Cyber Check for schools

Welcome

Arati Patel-Mistry
Cyber Security Engagement Lead

Department for Education

Today we will cover…

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

Please use the Q&A function to ask questions during the live event.
Slides will be sent to attendees after the presentation.

DFE Cyber Security Standards

1. Protect all devices on every network with a properly configured boundary or software **firewall**.
2. **Network devices** should be known and recorded with their security features enabled, correctly configured and kept up-to-date.
3. Accounts should only have the **access** they require to perform their role and should be authenticated to access data and services.
4. You should protect accounts with access to personal or sensitive operational data and functions by **multi-factor authentication**.
5. You should use **anti-malware software** to protect all devices in the network, including cloud-based networks.
6. An administrator should check the **security of all applications** downloaded onto a network.

Continued =>

7. All online devices and software must be **licensed** for use and should be patched with the **latest security updates**.

8. You should have at least **3 backup copies** of important data, on at least 2 separate devices, at least 1 must be off-site.

9. Your business continuity and disaster recovery plan should include a **regularly tested contingency plan** in response to a cyber attack.

10. **Serious cyber attacks should be reported**.

11. You must conduct a **Data Protection Impact Assessment** by statute for personal data you hold as required by General Data Protection Regulation.

12. **Train all staff with access** to school IT networks in the basics of cyber security.

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

PROJECT EVOLVE

Professionals Online Safety Helpline

360safe the online safety self-review tool

360earlyyears

Cyber Secure

SWGfL Safe. Secure. Online

SWGfL are a not-for-profit charity ensuring everyone can benefit from technology free from harm.

Part of the UK Safer Internet Centre, our experts advise schools, public bodies and industry, nationally and internationally. https://swgfl.org.uk

Jess McBeath
Online Safety & Security

INTERFACE

Revenge Porn Helpline

REPORT HARMFUL CONTENT

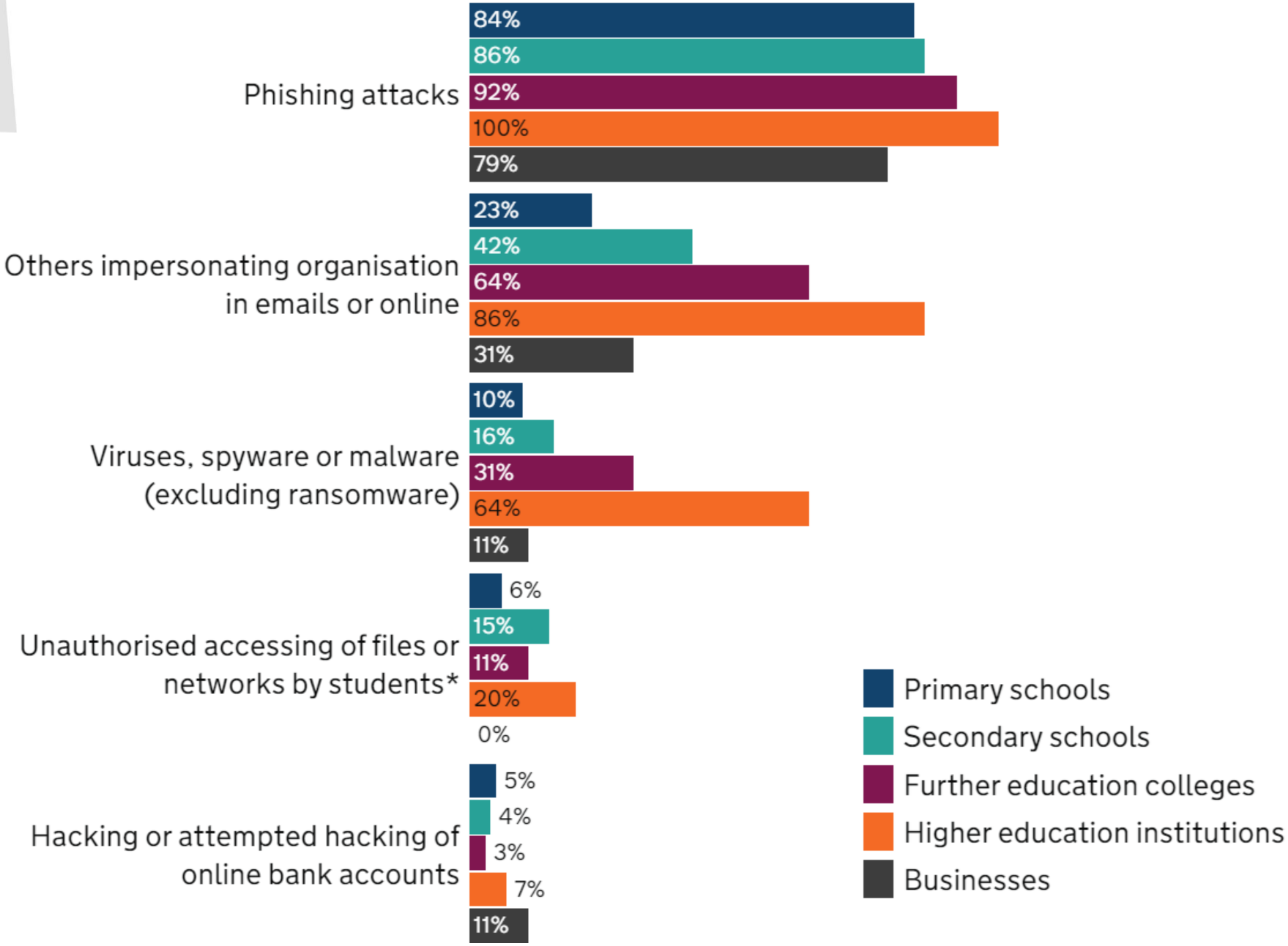
Test Filtering

ONLINE SAFETY live

CYBER THREAT

41% of primary and 63% of secondary schools identified cyber breaches or attacks 2022 – 2023*

Now add generative AI …



**DSIT Cyber Security Breaches Survey 2023*

CONTEXT AND IMPACT – SO WHAT?

Ransomware is the biggest threat facing the education sector

Over 80 incidents have been seen since August 2020

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

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

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 Uni student data to ransom
- Exams cancelled after Northumbria 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 shut

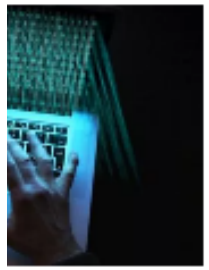
the potential impact of the attack

Each school associated with the t

Fears as 'thousands' of cyber attacks launched against British rsities

W

We



Most read in UK

SUBSCRIBE

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, affected schools are carrying out a data collection exercise. This would usually happen at the start

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

fe news.co.uk

HOME PUBLISH SEARCH

93% increase in cyberattack sector

fe news by Check Point Research Published: 23 August 2021 Hits: 125

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.

- 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.

Why we are contacting you?

The Department for Education and the National Cyber Security Centre (NCSC) has been made aware of an increasing number of cyber-attacks involving ransomware infection affecting the education sector at this time. The purpose of this letter is to make you aware of the threat and provide high-level information and advice to support your ongoing cyber security preparedness and mitigation work.

In all cases the NCSC has been working with the department and the affected providers to contain and support post-incident outcomes. However, these attacks and incidents have had a significant impact on the affected education provider's ability to operate effectively and deliver services.

These incidents appear to be financially driven but opportunistic, taking advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.

Whilst I would urge you to ensure that your systems, processes and awareness training are up to date, I also want to make you aware of the steps you should take if your educational setting is affected.

teiss News CISOs 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.

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

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

Cyber Secure

Department for Education/SWGfL

HOW DOES IT WORK?

https://CyberSecureCheckForSchools.uk

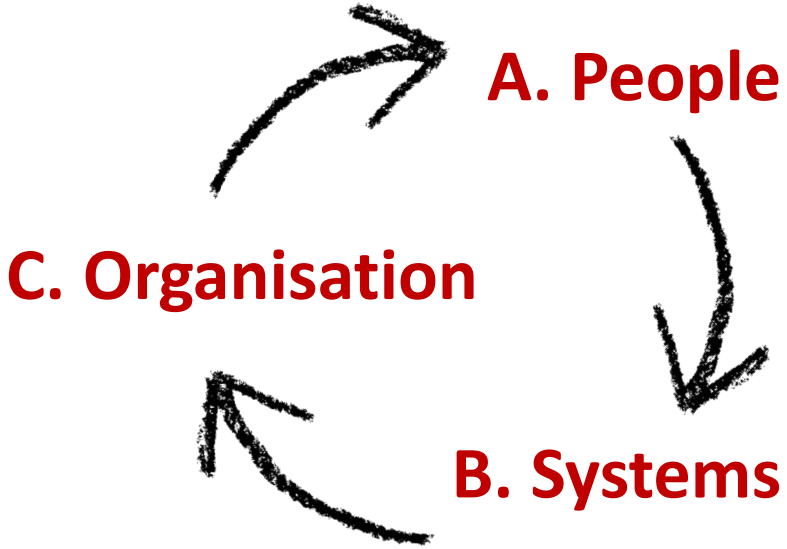
Grade your cybersecurity measures along 23 aspects

Anonymously compare performance with local/national averages

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

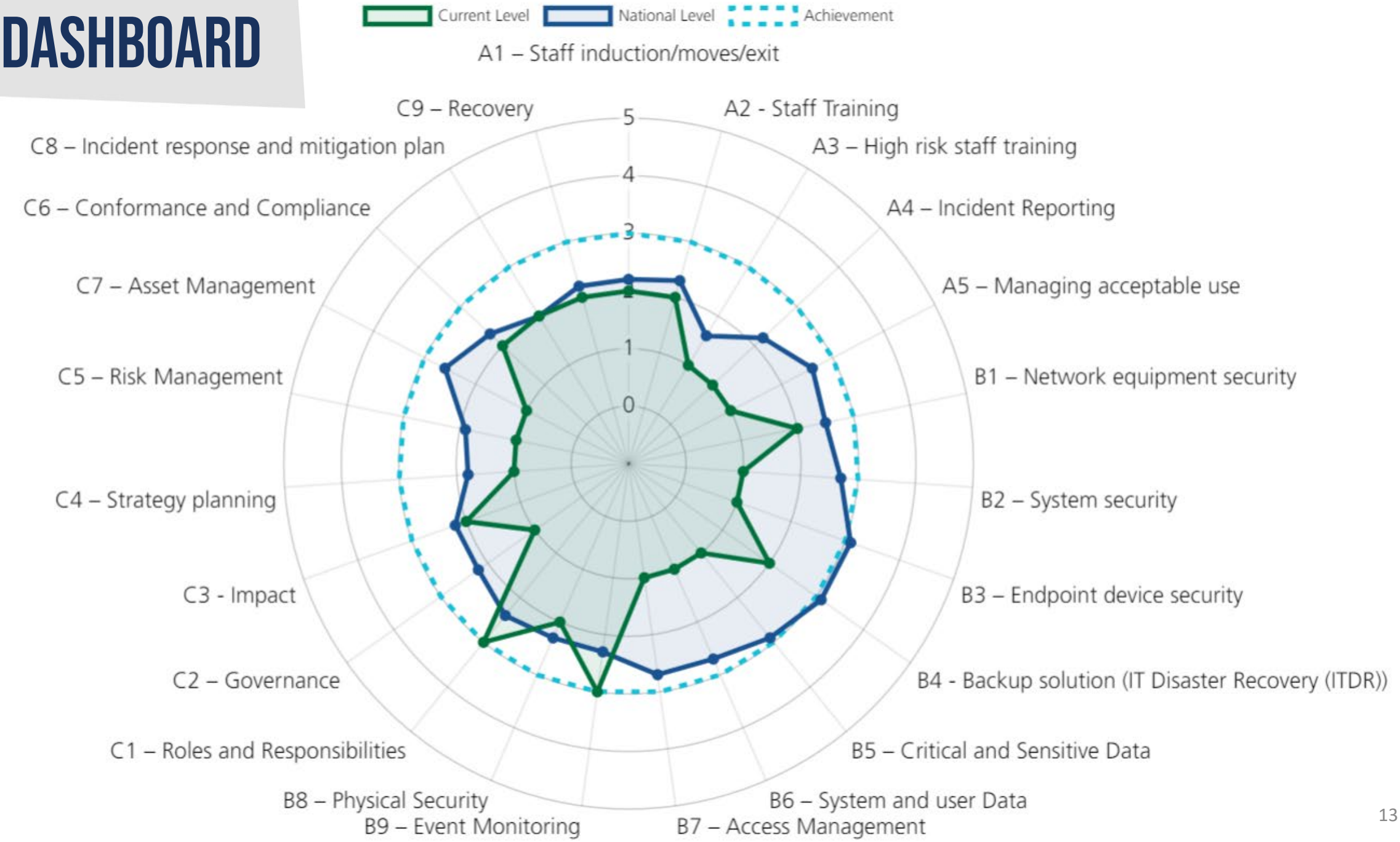
Includes guidance, templates and links to best practice resources

ASSESSMENT



Nothing in place	Minimal	Planning	Essentials *('Achievement')*	Effective	Outstanding
0	1	2	3	4	5

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

LINKS TO RESOURCES

Cyber Incident Contact List

Education Data Hub

Headteacher / Setting Lead:
Telephone:
Email:

Action Fraud
(Reporting Cyber Crime)
0300 123 2040 [Press 9 for active incidents]
https://www.actionfraud.police.uk/

NCSC Incident Reporting:
https://report.ncsc.gov.uk

Phishing Reporting:
report@phishing.gov.uk

Designated Safeguarding Lead

Name:
Telephone:

Cyber Protect Officer

Name:
Telephone:
Email:

Local Authority Designated Officer

IT Provision / Supplier

cyberIT Security Incident / Concern Form

Reference: Click or tap here

Names of all relevant staff / pupils concerned

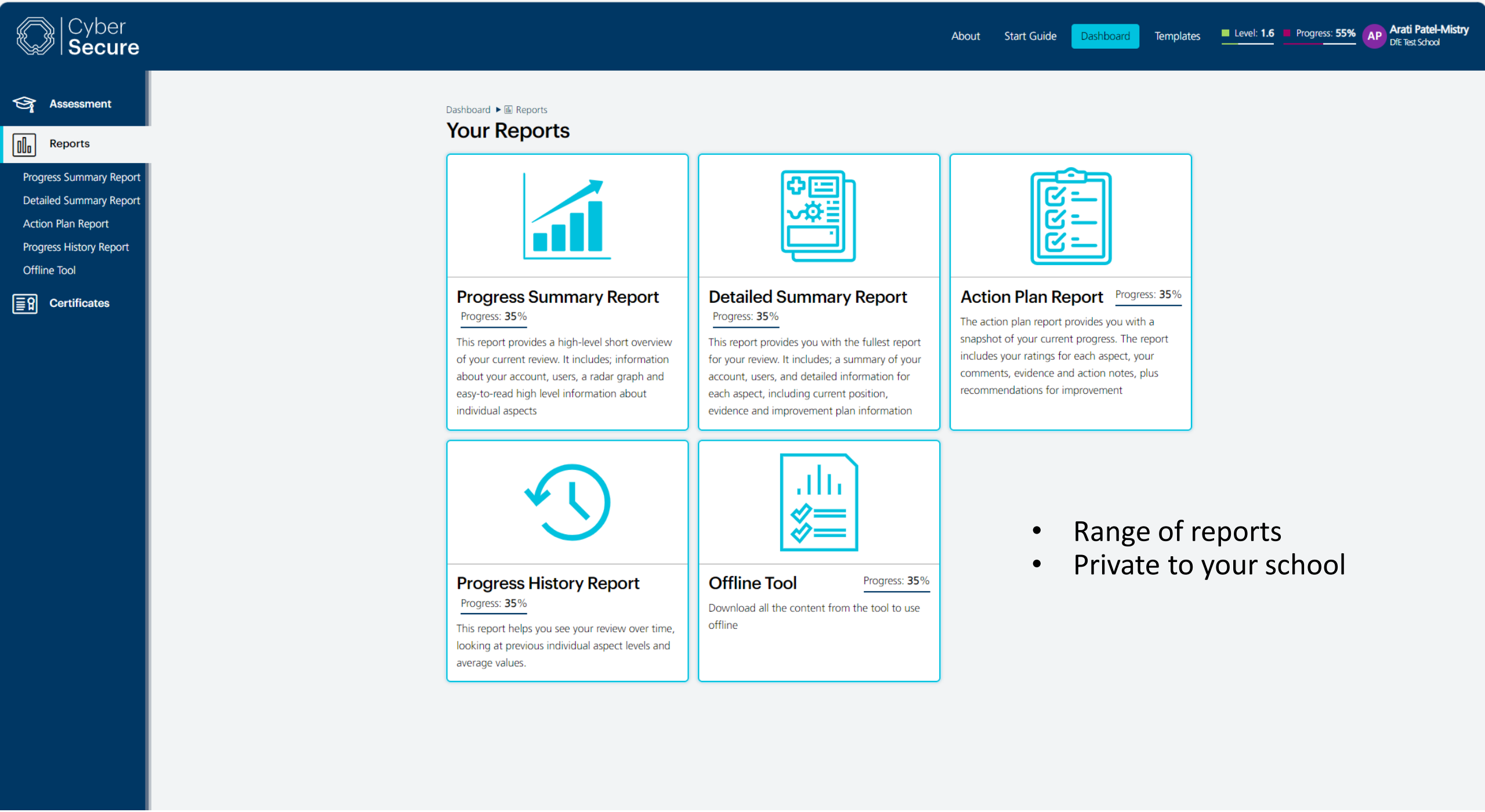
Click or tap here to enter text.

Date of Incident or Concern: Click or tap here **Time:** Click or tap here

Reported by: Click or tap here to enter text. **Role:** Click or tap here to enter text.

Is this incident a:

- ☐ **Safeguarding Concern**
- ☐ **Filtering Issue / Unsuitable Content**
- ☐ **Security Threat / Cyber-attack**
- ☐ **Virus / Malware Report**
- ☐ **Other**



- Range of reports
- Private to your school

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

THINGS TO THINK ABOUT

- Roles and responsibilities
- Timeframe
- Data
- Keeping Children Safe in Education
- Reports
- Other things to consider

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

Cyber Secure

Q&A

Cyber Secure Frequently Asked Questions

https://cybersecurecheckforschools.uk/faqs/

Goodbye & thank you for watching