WORSHIPFUL COMPANY OF INFORMATION TECHNOLOGISTS

Information Security Panel • Briefing Note

Cyber Resilience

A practical guide for charities, livery companies and schools

Why and how to protect your people, your data and your reputation from cyber incidents, in plain English.

Version 2.1 • October 2026

Drawing on the work of the WCIT Information Security Panel.

About this briefing

Cyber crime is no longer something that happens only to banks, governments and big corporates. The data is unambiguous: charities, livery companies and schools are now firmly in the firing line, and the threat is growing every year.

This briefing is written for the people who run those organisations: trustees, governors, court members, head teachers, business managers, charity CEOs and the volunteers who keep things going. You do not need to be a technologist to use it.

Our promise: no jargon for its own sake, no fear-mongering, and no "you must buy this product" advice. Where we do recommend a tool or scheme it is because it is free, government-backed, or widely used and trusted.

How to use this document

- If you have ten minutes, read the Executive Summary on page 3 and the checklist for your role in Part 5.
- If you have an hour, read it cover to cover. It is shorter than it looks.
- Then keep it on a shared drive, send it to your trustees, and use the checklists in your next governance meeting.

Who this is for

- City Livery Companies and the schools and charities they support.
- Independent and state schools, multi-academy trusts and further education colleges.
- Small and medium charities, foundations and grant-making bodies.
- Membership bodies, professional institutes and other not-for-profits.

Who wrote it

This briefing is published by the Information Security Panel of the Worshipful Company of Information Technologists (WCIT), one of the City of London's modern livery companies. The Panel brings together senior cyber security practitioners from industry, government and academia, all of whom volunteer their time.

It draws on guidance from the National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS), the Department for Education (DfE), City of London Police, IASME and the Cyber Resilience Centre for London.

What has changed in this edition (v2.1, October 2026)

- Statistics refreshed and correctly attributed to the government's Cyber Security Breaches Survey 2025/2026,published in April 2026.
- The Department for Science, Innovation and Technology (DSIT) was dissolved on 20 July 2026; government responsibility for cyber security and resilience now sits with DCMS.
- Action Fraud has been replaced by Report Fraud (December 2025). All reporting details are updated.
- Cyber Essentials was tightened in April 2026: MFA is now mandatory on every cloud service that offers it.
- New guidance for schools on the DfE cyber security standards, Risk Protection Arrangement conditions andincident reporting.
- New case study on the 2025 attack on a London nursery chain; British Library case study brought up to date.
- Legislative outlook updated: Cyber Security and Resilience Bill, ransomware measures and Computer MisuseAct reform.
- Awareness resources refreshed; corrected dates, contacts (Cyber Griffin, Police CyberAlarm) and typographical errors.

Disclaimer
WCIT assumes no responsibility or liability for any errors or omissions in the content of this document. The information contained in this document is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness or timeliness. It is written in good faith based on current knowledge and experience and is provided for guidance only. Specific actions, in particular legal, regulatory or insurance matters, should be taken with appropriate professional advice.

Executive summary | If you read nothing else, read this page

The threat in 2026

28%
of UK charities reported a cyber breach or attack in the last 12 months, around 57,000 organisations.

73%
of UK secondary schools identified a cyber breach or attack in the last 12 months, up from 60% a year earlier. For universities the figure is 98%.

204
nationally significant cyber incidents handled by the NCSC in the year to August 2025, more than double the previous year.

38%
of UK charities use any two-factor authentication. The most effective single defence is still missing in most.

$25M
lost by engineering firm Arup to a single AI deepfake video call impersonating its CFO.

82%
of phishing emails now contain AI-generated content. They are getting harder to spot.

Sources: UK government Cyber Security Breaches Survey 2025/2026; NCSC Annual Review 2025; press reports; independent industry analysis.

The five biggest risks for your organisation

1. Phishing emails and texts that trick a staff member, volunteer or trustee into handing over a password or clicking a malicious link.
2. Ransomware that locks your files, donor records or pupil data and demands payment to release them.
3. Business email compromise: fake invoices or fraudulent payment instructions that look as though they come from a trustee, the CEO or a known supplier.
4. Account take-over of cloud services such as Microsoft 365 or Google Workspace, often via a stolen or reused password, or an attack on a supplier who holds your data.
5. AI-enabled scams: deepfake voice or video calls impersonating a senior leader, and AI-written phishing in fluent, error-free English.

The five things to do this month

- Turn on multi-factor authentication (MFA) on every email, banking and cloud account, starting with the trustees, CEO and finance team.
- Sign your organisation up to Cyber Essentials, the UK government's baseline cyber security standard. It costs from £320 plus VAT and protects you against the great majority of common attacks.
- Make sure every important file is backed up to a separate, offline or cloud location, and test that you can actually restore it.
- Run a 30-minute awareness session for staff, volunteers and trustees, using the free NCSC material and WCIT videos listed in this briefing.
- Write a one-page incident response plan: who do you call, in what order, if your systems go down on a Sunday morning?

If you do nothing else…

Turn on Multi-Factor Authentication everywhere. The single biggest reason that small organisations fall victim to cyber crime is reused or stolen passwords. MFA (a code on your phone, a fingerprint or a hardware key) stops over 99% of common account-takeover attacks. It is free, it takes minutes, and it works. Since April 2026 it has also been mandatory for Cyber Essentials on every cloud service that offers it.

Part 1: Understanding the threat

Why this matters now

Over the last twenty years we have all become much more connected. That has brought enormous benefits, including access to information, easy collaboration, online giving and hybrid working, but it has also opened us up to a new class of risk that did not really exist a generation ago.

The numbers are stark. The government's Cyber Security Breaches Survey 2025/2026, published in April 2026 by the Home Office and DSIT (whose cyber security responsibilities passed to DCMS when DSIT was dissolved in July 2026), found that around 28% of UK charities had suffered a cyber breach or attack in the previous 12 months, roughly 57,000 organisations. Phishing was by far the most common attack, and around one in seven charities (14%, about 28,000) had been the victim of at least one cyber crime. For most, the direct cost of their worst breach was modest, but a minority faced much larger bills, and the survey can only count the attacks that organisations actually spotted.

Worryingly, the proportion of charities treating cyber as a high priority fell from 68% to 60%, its lowest level since 2017/18, driven by smaller charities. Only 17% of charities ran any staff training or awareness activity during the year, and only 38% use two-factor authentication.

Schools are even more exposed. The same survey found that 73% of secondary schools (up from 60% a year earlier), 88% of further education colleges and 98% of universities had identified a breach or attack in the past year. Even among primary schools the figure was 49%. Around one in ten secondary schools said they were attacked at least daily.

The National Cyber Security Centre's Annual Review 2025 reports a record 204 nationally significant incidents in the year to August 2025, more than double the 89 recorded the year before; 18 of them were classed as highly significant. The most pressing threat, by some distance, is ransomware.

2025 also showed how far the damage from a single attack can spread. The attack on Jaguar Land Rover, which halted its UK factories for around five weeks, is estimated by the independent Cyber Monitoring Centre to have cost the UK economy about £1.9 billion and to have affected more than 5,000 organisations in its supply chain. Attacks on Marks & Spencer and the Co-op caused weeks of disruption in the same year.

Who is the threat from?

Insiders

Disaffected staff, volunteers or contractors with legitimate access to your systems can divert information or funds. Insider risk is rarely malicious from day one. It is more often the gradual erosion of access controls, leavers whose accounts are not closed, or trusted people taking shortcuts.

Organised crime

This is the single largest source of attacks against organisations of your size. Criminal gangs, many operating from outside the UK, run cyber attacks as a business. Their goal is money: stealing it directly from your bank account, defrauding your suppliers, or encrypting your data and demanding a ransom in cryptocurrency. They work to office hours, have customer-service desks, and increasingly use AI to scale up.

Hostile states

State-sponsored actors from Russia, China, North Korea, Iran and elsewhere attack critical infrastructure, steal sensitive information and try to influence democratic processes through disinformation and "fake news". Most charities and livery companies are not direct targets, but high-profile schools, faith-based organisations, defence-adjacent charities and bodies that work with politically sensitive groups should assume they could be.

What has changed in this edition (v2.1, October 2026)

Cyber security marketing has long traded in Fear, Uncertainty and Doubt, the so-called "FUD". The point of this briefing is the opposite: the great majority of attacks succeed because of basic, fixable, human-scale failings. You do not need a six-figure security budget to be safe; you need a calm, sensible plan and the discipline to follow it.

Hacktivists, opportunists and the merely mischievous

Some attacks are not financially motivated at all, and some are carried out by people barely out of school. They may be retaliation for a perceived political stance, the work of a single dissatisfied beneficiary, or simply a pupil testing what they can get away with. Several damaging UK attacks in 2025, including the theft of nursery children's data described below, led to the arrest of teenagers. The defences are largely the same.
Who is the threat from?

Why should an attacker pick on us?

It is tempting to think "we are too small, too obscure, too low-budget to be a target". This is one of the most dangerous misconceptions in cyber security. The data tells a different story:

- Charities hold rich data: donor financial details, vulnerable beneficiaries' personal information, safeguarding files.
- Schools hold pupil records and parental bank details, and have predictable cash-flow patterns.
- Livery companies sit on substantial endowments and charitable funds, often administered by small lay teams.
- All three groups tend to have small IT functions, modest cyber budgets and stretched volunteer trustees, which makes them, in attackers' eyes, easier targets than a high-street bank.
- Your suppliers hold your data too. The cloud platforms, payroll bureaux, school information systems and fundraising databases you rely on can be attacked even when your own house is in order.

Most attacks today are not aimed at any one organisation. They are scattergun: millions of phishing emails, automated scans of every internet-facing system in the UK, opportunistic ransomware deployed wherever a foothold can be gained. The question is rarely "will we be attacked?" but "when our number comes up, will we cope?"

What's the worst that could happen?

In our sectors, a serious incident can mean any combination of:

- Financial loss: stolen funds, fraudulent payments, ransom demands, recovery costs.
- Reputational damage with donors, parents, pupils, members and beneficiaries.
- Regulatory exposure: the Charity Commission, Information Commissioner, Ofsted and Department for Education all take cyber incidents seriously.
- Operational paralysis: staff unable to access email, accounts, payroll or pupil records, sometimes for weeks.
- Wellbeing impact: trustees and senior staff dealing with a major incident routinely report serious stress, sleep loss and burnout.
- Existential risk: small organisations have closed as a direct consequence of a single attack.

Case study: The British Library, 2023

In October 2023 the British Library, a national institution and registered charity, was hit by ransomware. The attackers are believed to have entered through a third-party account on a server that lacked multi-factor authentication. Around 600GB of data, including HR files, was stolen and dumped on the dark web after the Library refused to pay.

The Library estimated rebuild costs of around £7 million, with a total economic impact of £13 million to £17 million. Recovery has taken years: by 2026 the Library had restored its main catalogue and was moving from recovery to wider digital renewal. The Information Commissioner's Office took no enforcement action and pointed to the Library's published review of lessons learned, but the human, financial and reputational cost has been profound.

The lesson: even well-resourced organisations get hit, and a single account without MFA was enough.

Case study: Kido nurseries, 2025

In September 2025 criminals stole the names, photographs, dates of birth and family contact details of around 8,000 children from Kido, a chain of London nurseries. Much of the data was held on a third-party childcare platform. The attackers demanded around £600,000 in Bitcoin, published some children's profiles online and contacted parents directly to increase the pressure. Two 17-year-olds were arrested within weeks.

The lesson: your data is only as safe as the weakest system it sits in, including your suppliers' systems, and attackers will deliberately exploit the distress of families.

How attacks happen

There are roughly four ways an attacker can hurt you, and each one has a corresponding defence:

1. Social engineering

By far the most common. The attacker manipulates a human, by email, text, phone, video call or in person, into doing something they shouldn't: clicking a link, opening an attachment, transferring money, or revealing a password.

This works because cyber criminals use the same techniques legitimate advertisers do. Their offers are urgent and time-bound, like the proverbial sofa sale that must end Sunday. They prey on excitement, fear of loss, fear of being found in the wrong, or simple politeness. "Are you at your desk? I need a quick favour", sent in the name of your CEO, has cost organisations millions. In 2025, criminals who telephoned IT help desks while posing as genuine staff were able to reset passwords and cause major disruption at well-known UK retailers.

If a stranger rang your doorbell offering a free iPad, you would have your suspicions. We need the same instinct online.

2. Technical exploitation

Out-of-date software, misconfigured systems and unpatched vulnerabilities give attackers a way in. NCSC data for the year to August 2025 linked just three vulnerabilities, in Microsoft SharePoint Server, Ivanti Connect Secure and Fortinet FortiManager, to 29 of the incidents it managed.

3. Stolen or reused credentials

Passwords leaked from one website are routinely tried against thousands of others. If you use the same password on your charity's email and a fitness app that gets breached, attackers will be in your email within hours. This is why MFA matters so much.

4. Denial of service

A Distributed Denial of Service (DDoS) attack floods a website with traffic until it collapses. Such attacks are usually disruptive rather than destructive, but they can take a school registration system or a charity donation page offline at the worst possible moment.

The new front line: AI-enabled attacks

Generative AI has changed the economics of cyber crime. Attackers can now produce flawless English-language phishing emails, clone voices from a thirty-second YouTube clip, and run real-time deepfake video calls. In early 2024 an employee in the Hong Kong office of UK engineering firm Arup transferred around $25 million after a video call with what appeared to be the company's CFO and other senior colleagues. Every face on the call was AI-generated.

Independent analysis suggests over 80% of phishing emails now contain AI-generated content, and around 40% of business email compromise messages are written largely by AI. The defence is the same as ever (verify, don't auto-trust) but the standard for what looks suspicious has shifted.

Part 2: What you can do as an individual

This section is the practical heart of the briefing. None of it requires technical skill. It is for everyone: trustees, staff, volunteers, members, parents, governors, choristers and beadles.

1. Use strong, unique passwords

Make passwords long. Length beats complexity. The NCSC recommends three random words, something like "coffee-brick-trumpet", because they are hard for computers to crack but easy for humans to remember.

- Never reuse a password. If one site is breached, every account using that password is exposed.
- Avoid anything a criminal could guess from your social media: pet names, birthdays, the schools you attended.
- Be wary of "what's your superhero name?"-style quizzes. They are sometimes harvesting password-recovery answers.
- Use a password manager: a dedicated app such as 1Password or Bitwarden, or the password manager built into your browser or phone. You only have to remember one strong master password.
- Where a website or app offers a passkey, use it. Passkeys replace the password altogether and are almost impossible to phish.
- Check your accounts at haveibeenpwned.com, a legitimate service that tells you whether your email or phone number has appeared in a data breach. If it has, change those passwords today.

2. Turn on multi-factor authentication everywhere

Multi-factor authentication (MFA) means you need more than just a password to log in. Typically it adds something you have (your phone, a security key) or something you are (a fingerprint, your face) to something you know (the password).

MFA stops over 99% of common account-takeover attacks. It is the single most effective thing you can do.

- Turn it on for your email first. If attackers control your email they can reset every other password.
- Then your bank, your charity's cloud accounts (Microsoft 365 or Google Workspace) and your social media.
- Prefer an authenticator app (Microsoft Authenticator, Google Authenticator) or a hardware key over SMS codes. SMS can be intercepted via SIM-swap attacks, though it is still much better than nothing.
- If your bank, school, charity or supplier doesn't offer MFA, ask why.

3. Turn on multi-factor authentication everywhere

Every update for your laptop, phone or tablet contains fixes for vulnerabilities that attackers actively exploit. Putting them off is a free gift to the bad guys.

- Turn on automatic updates for your operating system, browser and main applications.
- Don't ignore the pop-up that says "update available". Install it at the next sensible moment.
- Replace devices that no longer receive security updates. An old phone running unsupported software is a permanent open door. Windows 10 reached the end of support in October 2025: unless your organisation has paid for Extended Security Updates, upgrade or replace any PC still running it.
- Install reputable anti-virus or anti-malware software and let it update automatically. Microsoft Defender, built into Windows, is a perfectly good free starting point.

4. Be careful with email

Most attacks start with an email. Two simple habits stop the vast majority:

Check who the message is really from. The display name ("HMRC", "your CEO") can be anything. Hover over it, right-click or tap-and-hold to reveal the real address. "hmrc-refunds@strangedomain.com" is not HMRC.

Check where the link really goes. Hover over a link without clicking and the real destination appears. If the visible text says "Microsoft.com" but the real link is "microsoft-login.xyz", do not click.

- Be suspicious of urgency: "act now or your account will be closed", "this offer ends today", "I need a quick favour while I'm in a meeting".
- Be suspicious of unexpected attachments: invoices you weren't expecting, CVs from people you don't know, voicemail attachments.
- If in any doubt, ring the supposed sender on a number you already have, not the one in the email.

- Forward suspicious emails to the National Cyber Security Centre at report@phishing.gov.uk, and forward suspicious texts to 7726 (it spells SPAM). Since 2020 the public has reported more than 55 million suspicious emails this way, helping the NCSC remove over 250,000 scams.

5. Be careful on social media

Social media is gold for cyber criminals. They use it to research targets, impersonate trustees and chief executives, and to harvest the answers to your password-recovery questions.

- Tighten your privacy settings on every platform. Make sure your posts, friend list and profile are visible only to people you actually know.
- Think before you check in to locations, post live holiday photos, or share your daily commute. You are telling fraudsters when you are not at home.
- Don't trust adverts on social media just because the platform is mainstream. Bargains, job offers and investment schemes are routinely fraudulent.
- Treat "follow request" notifications from people who already follow you as a likely impersonation

6. Watch out for QR codes and harmful apps

Criminals print fraudulent QR codes onto stickers and place them over genuine ones on parking meters, restaurant tables, leaflets and posters. The fake code takes you to a lookalike site that captures your card details or installs malware.

- Look for signs the QR code has been tampered with: a sticker over another sticker, an oddly clean code on a weathered sign.
- Where possible, type the web address into your browser yourself rather than scanning.
- Only install apps from the official Apple App Store or Google Play. Be suspicious of any app that asks for accessibility permissions, which let it see and control everything on your device.

7. Be alert to phone scams

Reputable organisations such as your bank, HMRC, the police and your phone provider will not:

- Call and ask you to read out a one-time passcode or security code.
- Tell you to ignore security warnings on your device.
- Get angry if you say you'd rather hang up and ring them back on the number on their website.
- Pressure you into making a payment, transferring money, or installing remote-access software in a single phone call.

8. Be careful on social media

Until recently, hearing your CEO's voice or seeing them on a video call was reasonably good evidence that you were really talking to them. That is no longer true.

- Tighten your privacy settings on every platform. Make sure your posts, friend list and profile are visible only to people you actually know.
- Think before you check in to locations, post live holiday photos, or share your daily commute. You are telling fraudsters when you are not at home.
- Don't trust adverts on social media just because the platform is mainstream. Bargains, job offers and investment schemes are routinely fraudulent.
- Treat "follow request" notifications from people who already follow you as a likely impersonation

9. Secure your home network

Most of us now work, learn and donate from home networks that we never really set up properly.

- Change the default admin password on your router (the one written on the bottom). Use a long, unique password.
- Make sure your Wi-Fi uses WPA2 or WPA3 encryption.
- Set up a separate "guest" network for visitors and smart-home devices, so a compromised doorbell can't reach your work laptop.
- Update your router's firmware periodically. Your provider's app will usually do this for you.

10. Step away from the device

Many of the worst decisions are made in the moment, in a hurry, on a phone. The single most powerful trick is to give yourself five minutes.

> **Five-minute rule**
>
> If a message, call or pop-up is making you feel rushed, scared or excited, stop. Put the phone down. Make a cup of tea. Call the person back on a number you already have. The vast majority of scams rely on you not doing this. Almost nothing legitimate requires you to act in the next sixty seconds.

Part 3: What your organisation should do

Everything in Part 2 applies tenfold to organisations, because organisations are made up of individuals, each of whom can either let an attacker in or keep them out. Investing in firewalls and email filters matters, but it is no substitute for a culture of healthy scepticism. The actions below are pragmatic, proportionate and largely free or low-cost.

1. Educate your people

Cyber awareness is not a one-off training video. It is an ongoing conversation. Only 17% of charities ran any cyber training or awareness activity last year.

- Run a 30-minute briefing for staff, volunteers and trustees once a year, plus a short refresher for new joiners.
- Use free resources: the NCSC's posters and infographics (ncsc.gov.uk/section/infographics/home), its Cyber Aware campaign, its free cyber security training for school staff, and WCIT's own short awareness videos featuring the Beadle (see Resources and contacts).
- Run an occasional simulated phishing exercise, but use it to teach, not punish. The aim is for someone who clicks to feel safe reporting it, not embarrassed.
- Make it explicit and well known: nobody will ever be in trouble for raising the alarm about a possible incident.

2. Back up your data, and test the backups

Many of the organisations crippled by ransomware found, too late, that their backups were out of date, on the same network as everything else, or had never been tested. The widely used standard is the 3-2-1 rule:

The 3-2-1 backup rule

- 3 copies of every important piece of data.
- 2 different types of media or storage.
- 1 of which is offline or off-site: something an attacker who breaches your network cannot reach.

- For most charities, livery companies and schools the easiest answer is a reputable cloud back-up service for your Microsoft 365 or Google Workspace data, plus a separate copy of critical files (donor database, payroll, pupil records) on encrypted storage held off-site.
- Make at least one copy immutable, meaning it cannot be changed or deleted once written, so that ransomware cannot encrypt your backups as well.
- Test a restore at least twice a year. If you have never tried to restore a backup, you don't really have a backup. You have a hope.

3. Anti-virus, secure email and standard hygiene

- Install reputable anti-virus or endpoint software on every device that touches your network. Microsoft Defender for Business and the equivalents from Google, Sophos, ESET and others are all good.
- Use a cloud email service (Microsoft 365, Google Workspace) and turn on its built-in anti-spam, anti-phishing and attachment-scanning features. They are vastly better than anything an in-house mail server can offer.
- Apply software updates promptly across all devices and servers, including mobile phones.
- Maintain an up-to-date inventory of who has access to what. Disable accounts the day someone leaves. Quarterly access reviews are a good discipline.
- Limit "admin" rights to those who genuinely need them. Most users do not need to be local administrators on their laptop.
- Ask your IT provider and other key suppliers how they protect your data and whether they hold Cyber Essentials. Fewer than one in ten charities currently review the cyber risks posed by their suppliers.

4. Get certified to Cyber Essentials

- Cyber Essentials is the UK government's minimum baseline standard for cyber security, delivered by IASME on behalf of the NCSC. See iasme.co.uk/cyber-essentials.
- It is a verified self-assessment, marked by a qualified assessor, that confirms five technical controls: firewalls, secure configuration, user access control, malware protection and security update management.

- The requirements were tightened from 27 April 2026. MFA must now be switched on for every cloud service that offers it, cloud services can no longer be left out of scope, and critical or high-risk security updates must be applied within 14 days. Failing any of these means failing the assessment.
- Pricing for 2026 is unchanged: from £320 plus VAT for organisations with fewer than 10 staff, rising to £600 plus VAT for those with 250 or more. Organisations with a turnover under £20 million that certify their whole organisation also receive free cyber liability insurance.
- IASME offers free preparation material and a readiness tool, and some NCSC-assured Cyber Advisors offer eligible small organisations a free 30-minute session.
- It is increasingly required to bid for government, local authority and major funder contracts, and further education colleges must hold it under their funding agreement. Yet only 16% of charities have heard of it, and only 3% hold it.
- Cyber Essentials Plus adds an independent technical audit and is worth aiming for once you have the basics in place.

5. Consider cyber insurance, carefully

- Cyber insurance can cover first-party costs (recovering data, investigating the incident, reputation management, ransom payments where lawful) and third-party costs (claims by people whose data was lost). Around a third of charities (35%) have any form of cyber cover, usually as part of a wider policy.
- Premiums vary widely. Insurers will often require Cyber Essentials and MFA before they offer cover, and may refuse to pay out if your basic hygiene is poor.
- Read the exclusions carefully. “State-sponsored” carve-outs, social-engineering exclusions and warranty clauses are common pitfalls.
- Do not assume your existing professional indemnity, trustee or general liability cover protects you from cyber loss. Get specific advice.
- State-funded schools in England can get cyber cover through the DfE’s Risk Protection Arrangement (RPA). Cover depends on four conditions: offline backups; NCSC cyber security training each year for all staff and governors with access to IT systems; registration with Police CyberAlarm; and a written cyber response plan.

6. Have an incident response plan

Treat a cyber incident the way you treat a fire alarm. The plan does not need to be long or elaborate; it does need to exist before it is needed, and the people in it need to have read it. Only 19% of charities have a formal incident response plan; schools do much better, at 73% of primary and 77% of secondary schools.

A good plan answers, on a single side of A4:

- Who is in charge in the first hour? Who is the deputy if they are unreachable on a Sunday morning?
- Which third-party numbers do we ring? IT support, lawyers, the insurer’s incident hotline (or the RPA emergency helpline for schools), Report Fraud on 0300 123 2040, the Cyber Resilience Centre for London.
- How do we communicate if our email and phones are down? (Hint: have an out-of-band channel, such as a WhatsApp group on personal phones, or a couple of separate email accounts with their details kept in a sealed envelope.)
- Who do we have to notify? The Information Commissioner (within 72 hours for personal data breaches), the Charity Commission, the Department for Education, Ofsted, banking partners, key donors, members.
- Where are our backups? How do we restore? Who knows the master passwords?
- What is our holding line for media, parents, members and the public?
- Practise it. Cyber Griffin, run by City of London Police, offers free tabletop incident-response exercises to City businesses and Livery Companies and their associated charities and schools (cybergriffin.police.uk). The NCSC’s free Exercise in a Box lets you run one yourself.

7. Don't forget physical security

Cyber and physical security are no longer separate disciplines. The most sophisticated firewall is no use if a thief walks out with the laptop, or a visitor photographs the password on a sticky note.

- Lock your screen the moment you walk away from your desk: Windows key + L, or Ctrl + Cmd + Q on a Mac.
- Use full-disk encryption on every laptop and phone. Apple, Microsoft and Google all offer this for free.
- Keep paper records securely. Shred sensitive documents. Keep visitor logs.
- Think about who has the keys to your server cupboard. In many small organisations the PAT-tested kettle is governed more carefully than the networking equipment.
- Train front-of-house staff to challenge tail-gaters and unannounced "IT engineers".
- Be aware of physical-world risks linked to politics, faith or beneficiaries: bomb threats, swatting, doxxing, harassment of trustees. The Charity Commission's safeguarding guidance is the right place to start.

8. Get the governance right

Cyber security is a board responsibility, not something to delegate to a part-time IT manager or an external supplier. Yet only 30% of charities have a trustee with explicit responsibility for it.

- Put cyber risk on the board agenda at least twice a year, and on the audit committee agenda quarterly.
- Identify a named trustee with responsibility for digital and cyber. They do not need to be a technologist; they need to be willing to ask sensible questions.
- Include cyber on the strategic risk register and review it at least annually.
- Ensure your cyber insurance, supplier contracts and acceptable-use policies are reviewed and current.
- Use the government's Cyber Governance Code of Practice (April 2025) and the NCSC's free Cyber Security Toolkit for Boards, both written for non-technical trustees and directors.
- Schools and colleges should also follow the DfE's cyber security standards, which expect a cyber risk assessment every year, reviewed each term, and at least one governor or trustee to complete cyber training.

Part 4: If the worst happens

First: don't panic. The vast majority of incidents are recoverable. The single most common mistake is to make things worse in the first hour through a rushed, uncoordinated response.

If you are an individual and think you have been compromised

1. If you fear your bank account or card has been exposed, ring your bank immediately on the number on the back of your card.
2. Change passwords on any account you think might be affected, starting with your email. If you reused that password elsewhere, change it everywhere.
3. Turn on multi-factor authentication if you haven't already.
4. Run a full anti-virus scan on your device. If you cannot remove what you find, take it to a professional.
5. Forward the offending message to report@phishing.gov.uk, or forward suspicious texts to 7726.
6. Report the crime to Report Fraud on 0300 123 2040 or at reportfraud.police.uk (in Scotland, call Police Scotland on 101). The police cannot help with crimes they don't know about.
7. Tell the people in your life. The shame around being scammed is one of the criminals' best weapons; talking about it protects others and helps you recover.

If your organisation is compromised

A common, sensible sequence, based on the NCSC's incident-response guidance, is:

Identify

- What systems and data appear to be affected? When did it start?
- Which users, devices and accounts are involved?
- Is the incident still active, or has the attacker already left?

Contain

- Disconnect affected devices from the network, but do not turn them off, as this can destroy forensic evidence.
- Reset passwords for affected accounts and revoke their active sessions.
- Block known malicious senders and quarantine offending emails.

Eradicate

- Remove malware and unauthorised access, ideally with the help of a qualified incident-response firm.
- Patch the vulnerabilities that were exploited.
- Change all administrative credentials.

Recover

- Restore systems from clean backups.
- Monitor closely for at least a fortnight. Attackers often try again.
- Confirm that all accounts and devices are accounted for.

Communicate

- Tell your insurer's incident hotline (or, for schools, the RPA emergency helpline) as early as possible. Some policies have very short notification windows.
- Report the attack to Report Fraud. If you are under a live attack, phone 0300 123 2040 rather than reporting online, so that specialist teams can act quickly.
- Notify the Information Commissioner's Office within 72 hours of becoming aware of a personal data breach if it is likely to result in a risk to individuals.
- Charities: submit a Serious Incident Report to the Charity Commission. Schools and colleges: report to your insurer or RPA, to Report Fraud and to the DfE sector cyber team (sector.incidentreporting@education.gov.uk), and to Ofsted where relevant.
- Report serious incidents, such as those causing long-term closure or significant financial damage, to the NCSC at report.ncsc.gov.uk.

Learn

- Hold a no-blame review after the dust settles. What worked? What didn't? What would have been impossible without the response plan?
- Update your plan, your policies and your training accordingly.

Should we pay a ransom?

- There is no guarantee the criminals will release your data, and many do not.
- Paying funds further attacks against others.
- Paying a sanctioned group, or one linked to one, may be a criminal offence in itself.
- Insurers may refuse to reimburse the payment.
- Once you have paid, you are known as someone who pays. Repeat attacks are common.

The government has also confirmed that it intends to ban public sector bodies, including state-funded schools, from paying ransoms, and to require other victims to report ransomware attacks and notify the authorities before any payment. It has said the National Security Bill, announced in the King's Speech in May 2026, will include measures to tackle ransomware. These rules were not yet law at the time of writing, but state schools and colleges should already plan on the basis that paying will not be an option.

If you are facing this decision, take legal advice immediately and engage your insurer and the police. The Cyber Resilience Centre for London and the No More Ransom project (nomoreransom.org) can sometimes help with free decryption tools.

Reporting and legal recourse

- What systems and data appear to be affected? When did it start?
- Which users, devices and accounts are involved?
- Is the incident still active, or has the attacker already left?

Cyber crime in the UK is principally covered by the Computer Misuse Act 1990 (which the government plans to update) and, for personal data, by the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

- Report Fraud, run by City of London Police, replaced Action Fraud in December 2025 as the national reporting service for fraud and cyber crime in England, Wales and Northern Ireland: reportfraud.police.uk, or 0300 123 2040.
- City of London Police is the national lead force for fraud and cyber crime and the first point of contact for City Livery Companies: cityoflondon.police.uk.
- Cyber Griffin, the City of London Police's specialist team, offers free briefings, threat assessments and tabletop exercises to City businesses and the Livery: cybergriffin.police.uk.
- The Cyber Resilience Centre for London is a police-led, government-funded not-for-profit, working with the Mayor's Office for Policing and Crime, that supports SMEs and third-sector organisations across Greater London. Membership is free: londoncrc.co.uk.
- The Information Commissioner's Office handles personal data breach reporting and regulates the UK GDPR: ico.org.uk.

Part 5: Checklists by role

Photocopy these. Put them in board packs. Tick them off..

Checklist for the Board, Court or Trustees

Strategic ownership	We have a named individual at board level with responsibility for cyber and digital risk.
Risk register	Cyber risk appears on our strategic risk register and is reviewed at least annually.
Board agenda	Cyber security is on the main board agenda at least twice a year.
Investment	We have a written, costed cyber security plan, proportionate to the size and risk profile of the organisation.
Insurance	We hold appropriate cyber insurance (or, for schools, meet the RPA cyber conditions), or have made an explicit decision not to.
Cyber Essentials	We are certified to Cyber Essentials under the current (April 2026) requirements, or have a dated plan to be.
Incident response	We have a written incident-response plan; the board has seen it; we have tested it in the last 12 months.
Reporting lines	Trustees know who to ring, in what order, on a Sunday morning.
Supplier risk	Our key technology suppliers (IT support, cloud, payroll, finance, fundraising, school information systems) have been reviewed for cyber maturity.
Culture	Staff and volunteers know how to report a suspected incident and feel safe doing so.
Trustee training	All trustees have completed at least basic cyber-awareness training in the last 12 months.
External assurance	We have an independent view (internal audit, an external review or a peer assessment) of our cyber posture.

Checklist for Management

Asset register	We know what hardware, software, cloud services and data we hold, and where.
MFA everywhere	Multi-factor authentication is enabled on all email, banking, finance, fundraising and admin accounts, and on every cloud service that offers it.
Patching	Operating systems, browsers and key applications update automatically; critical and high-risk updates are applied within 14 days; we know what is unsupported, and why.
Backups	We follow the 3-2-1 rule, with at least one offline or immutable copy. We have tested a real restore in the last six months.
Access control	Joiners, movers and leavers are processed promptly. Quarterly access reviews are documented.
Anti-malware	Reputable endpoint protection runs on every device, with regular updates.
Email security	Our email platform's anti-phishing, anti-spam and attachment-scanning features are switched on.
Monitoring	We are registered with Police CyberAlarm and the NCSC's free Early Warning service.
Awareness	Every member of staff and every volunteer has had cyber awareness training in the last 12 months.
Phishing simulation	We run periodic simulated phishing exercises and use them constructively.
Policy suite	We have written, current policies for acceptable use, passwords, BYOD, remote working and incident response.
Vendor management	Cyber clauses are included in supplier contracts and reviewed at renewal.
Physical security	Devices are encrypted, screens lock automatically, and server rooms and cabinets are physically secured.
Reporting	We know how to report incidents internally, to Report Fraud, to the ICO and to our regulators.

Checklist for individuals: staff, volunteers, trustees, members

Passwords	I use long, unique passwords (or three random words), or passkeys, on every account.
Password manager	I use a password manager so I don't have to remember them all.
MFA	I have multi-factor authentication switched on for email, banking and any work accounts.
Updates	My laptop and phone install updates automatically, and still receive them.
Anti-virus	I run reputable anti-virus or anti-malware software on my devices.
Phishing	I check who emails are really from and where links really go before I click.
7726 / report@phishing	I know to forward suspicious texts to 7726 and emails to report@phishing.gov.uk.
Social media	My personal social media accounts are set to private; I am sparing about what I post.
QR codes	I am wary of QR codes in public places and prefer to type web addresses into the browser.
Phone scams	I never read out one-time passcodes; I hang up and call back on a trusted number.
Voice / video	I have agreed a callback procedure with my team for any unusual money or data request, even from people I know.
Devices	My laptop and phone lock automatically when I walk away. I don't leave them in cars or cafés.
Home Wi-Fi	I have changed the default password on my router and use WPA2 or WPA3 encryption.
When in doubt	I report anything suspicious. Nobody will be cross with me for asking.

Part 6: What does the future hold?

Technology evolves rapidly, and criminals are early adopters of every tool that comes along. Three trends are worth watching.

AI on both sides

Generative AI is already transforming the economics of cyber crime: better-written phishing, deepfake voice and video, automated reconnaissance. But it also gives defenders much better tools: anomaly detection, automated triage, summarisation of vast log files. Expect AI to be embedded in every mainstream security product within the next two years.

Identity and the end of the password

Major platforms are moving towards "passkeys": cryptographic credentials stored on your devices that replace the password entirely. They are far more secure, easier to use and almost impossible to phish. Expect them to become the default for cloud services during 2026 and 2027. The DfE's cyber standards for schools already recognise passkeys as an alternative to traditional MFA on dedicated devices.

Regulation will tighten

- The Failure to Prevent Fraud offence, in force since September 2025, makes large organisations criminally liable if an associated person commits fraud for the organisation's benefit and reasonable prevention procedures were not in place.
- The Cyber Security and Resilience Bill completed its Commons stages in June 2026 and is now before the House of Lords. It will bring managed IT service providers, including many of the outsourced IT support firms used by charities and schools, into regulation, and give regulated organisations 24 hours to make an initial report of a significant incident. Since DSIT was dissolved in July 2026, government responsibility for cyber security and resilience, including this Bill, has sat with DCMS.
- The National Security Bill, announced in May 2026, is expected to update the Computer Misuse Act 1990 and to take forward the government's plans on ransom payments and mandatory ransomware reporting.
- Rules on AI use, deepfake disclosure and personal data handling will continue to develop.

Charities, livery companies and schools should expect more, not less, scrutiny.

A final word

There is no such thing as absolute cyber security. But by following the advice in this document you can avoid the vast majority of the cyber crime your organisation is likely to encounter. The basics matter, the basics work, and the basics are mostly free.

Once you have done these things for your charity, your livery company or your school, do them for your family, your friends and your wider community. The strongest cyber-resilient society is one in which the basics are in everyone's toolkit.

Glossary

APT	Advanced Persistent Threat. A well-resourced criminal or state-sponsored group that researches its targets and conducts sophisticated, sustained attacks.
BEC	Business Email Compromise. Fraud carried out by impersonating a senior executive, supplier or trustee in email, typically to redirect a payment.
Botnet	A network of compromised devices, controlled by an attacker, used to launch larger attacks against others.
Cyber Essentials	The UK government-backed certification, delivered by IASME on behalf of the NCSC, that covers basic cyber hygiene. Increasingly required to bid for public sector contracts.
DDoS	Distributed Denial of Service. An attack that floods a website or service with traffic until it stops working.
Deepfake	A video, image or audio clip generated or altered by AI to convincingly impersonate a real person.
Malware	Malicious software, including viruses, spyware, stalkerware, scareware and ransomware. Multi-Factor Authentication. Requiring more than one type of evidence (typically a password plus a code on your phone or a fingerprint) to log in.
MFA	Managed Service Provider. An outside company that runs or supports your IT, and therefore often holds privileged access to your systems.
MSP	A modern, passwordless credential stored on a device. Far more secure and easier to use than a password.
Passkey	A software update that fixes a bug or security vulnerability.
Patch	A fake email, text, call or website that tries to trick the recipient into revealing information or installing software.
Phishing	Malware that locks or encrypts your data, then demands payment to release it. Often combined with theft of the data and a threat to publish it.
Ransomware	An attack in which a fraudster persuades a mobile operator to transfer the victim's phone number to a SIM they control, letting them intercept SMS-based MFA codes.
SIM-swap	Phishing by text message (SMS).
Smishing	The art of manipulating people into doing things they shouldn't. It underlies most cyber crime.
Social engineering	An attack that reaches you through a supplier, such as your IT provider or a cloud platform that holds your data.
Supply-chain attack	Malware disguised as something legitimate: a useful application, an attachment, an update. Phishing by voice call, including AI voice-clone attacks.
Trojan	A previously unknown vulnerability, for which no patch yet exists.
Vishing	I report anything suspicious. Nobody will be cross with me for asking.
Zero-day	I have changed the default password on my router and use WPA2 or WPA3 encryption.

More terms? The NCSC has a comprehensive glossary at ncsc.gov.uk/information/ncsc-glossary.

Resources and contacts

Government, regulators and police

- National Cyber Security Centre: ncsc.gov.uk. The UK government's authoritative source. Start with the Small Charity Guide, the Small Business Guide and the Cyber Security Toolkit for Boards.
- NCSC Cyber Action Toolkit: free, personalised step-by-step actions for sole traders and small organisations, a good first step towards Cyber Essentials: cybertoolkit.service.ncsc.gov.uk.
- NCSC Exercise in a Box and Early Warning: free services to rehearse your incident response (ncsc.gov.uk/information/exercise-in-a-box) and to be alerted to malicious activity on your network (ncsc.gov.uk/information/early-warning-service).
- Cyber Aware (NCSC): ncsc.gov.uk/cyberaware/home. Plain-English advice for individuals.
- Cyber Essentials (IASME / NCSC): iasme.co.uk/cyber-essentials.
- Department for Digital, Culture, Media and Sport (DCMS): gov.uk/government/organisations/department-for-digital-culture-media-and-sport. The lead government department for cyber security and resilience policy since DSIT was dissolved in July 2026.
- Cyber Security Breaches Survey 2025/2026: gov.uk/government/statistics/cyber-security-breaches-survey-20252026.
- Report Fraud: reportfraud.police.uk, or 0300 123 2040. Replaced Action Fraud in December 2025.
- City of London Police: cityoflondon.police.uk. The national lead force for fraud and cyber crime.
- Cyber Griffin: cybergriffin.police.uk. City of London Police's specialist team supporting City businesses and Livery Companies.
- Cyber Resilience Centre for London: londoncrc.co.uk. A police-led, government-funded partnership for SMEs and the third sector across Greater London.
- Information Commissioner's Office: ico.org.uk. Personal data breach reporting and UK GDPR guidance.

Sector-specific guidance

- Charity Commission: gov.uk/government/organisations/charity-commission. Serious incident reporting, trustee duties, safeguarding.
- Charity Digital: charitydigital.org.uk. Free and discounted technology and cyber services for charities.
- DfE cyber security standards for schools and colleges: gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges.
- DfE Cyber Security Hub: cyber-security-hub.education.gov.uk. Including the Risk Protection Arrangement cyber conditions.
- NCSC cyber security training for school staff: ncsc.gov.uk/information/cyber-security-training-schools.
- Jisc: jisc.ac.uk. Cyber services for further and higher education.

Awareness and learning

- WCIT short videos featuring the Beadle: "Password Idiot" (youtube.com/watch?v=NzHhKBARvo0); "Trapped", on software updates (youtube.com/watch?v=eMmDcfUF6g8); "Link Clicker", on phishing (youtube.com/watch?v=CbhE2h0QHRA).

Tools and self-checks

- Have I Been Pwned: haveibeenpwned.com. Has my email or phone number been involved in a breach?
- No More Ransom: nomoreransom.org. Free decryption tools for many ransomware strains.
- Police CyberAlarm: cyberalarm.police.uk. A free, Home Office-funded monitoring service for businesses, charities and schools, relaunched on a new platform in June 2026.

Privacy and security settings on social media

- Facebook: facebook.com/help/235353253505947
- Instagram: help.instagram.com/369001149843369
- TikTok: tiktok.com/safety/en/privacy-and-security-on-tiktok
- Snapchat: help.snapchat.com/hc/en-gb/articles/7012304746644

Reporting suspicious messages

- Suspicious emails: forward to report@phishing.gov.uk.
- Suspicious texts: forward to 7726 (which spells SPAM).
- Suspicious phone calls: text the word "Call" followed by the number to 7726.
- Fraud or attempted fraud: Report Fraud on 0300 123 2040 or reportfraud.police.uk.

About WCIT

The Worshipful Company of Information Technologists is the 100th livery company of the City of London. WCIT supports its associated charities, schools and the wider London community through philanthropy and expert volunteering. Through its Information Security Panel, and its partnership with City of London Police, IASME and the Cyber Resilience Centre for London, it helps the third sector to become more cyber resilient.

If you have feedback on this briefing, or would like to suggest improvements for the next edition, please contact the WCIT Information Security Panel via the WCIT website (wcit.org.uk/contact).

© 2026 The Worshipful Company of Information Technologists.
May be reproduced and distributed freely, with attribution, for non-commercial educational purposes.