

DPO NEWSLETTER

In this issue

- [Cyber Security Awareness Month October 2026](#)
- [Cyber Security in Schools: Key Lessons from the 2025/26 Survey](#)
- [DPIAs: Start Early, Avoid the Last-Minute Rush](#)
- [New Resources Available](#)
- [Keeping Templates Up to Date](#)
- [Compliance Review Process for 2026/27](#)
- [Stay Connected](#)

We hope that you find this issue to be an interesting read and, as always, our team is here to support you. If you have any questions or concerns, please do not hesitate to get in touch:

✉ l-west@bathnes.gov.uk ☎ 01225 395 959

● Cyber Security Awareness Month October 2026

Is your school cyber aware?

Well-informed staff and pupils are one of the strongest lines of defence against cyber incidents. Ideally trusts, schools, and colleges should have a clear plan about how to raise cyber awareness in the school, supported by an up-to-date IT Security Policy, an Acceptable Use Policy, and regular training.

More information can be found within the Department for Education's (DfE) core standard:

[Meeting digital and technology standards in schools and colleges](#)

For Cyber Security Awareness Month this October, you are encouraged to:

- Review your Acceptable Use Policy and ensure it covers staff, pupils, governors, supply staff, agency workers, and other users who access the network or data.

- Provide cyber security training at least annually for relevant adults, with additional training where particular risks have been identified. The DfE has broadened its digital and technology standards to also include cyber training for pupils.
- Monitor risks associated with phishing, online safety, social engineering, device security, password security, multi-factor authentication, data protection, and incident reporting.
- Make sure staff and pupils know how and when to report cyber incidents and personal data breaches.
- Involve key colleagues, including the schools SLT digital lead, IT support, data protection lead and DSL, so that they work together to resolve cyber security, data protection, and safeguarding issues.
- Consider ways of raising cyber awareness among parents and families, particularly where school devices are taken home or pupils access learning online.

For schools using the DfE Risk Protection Arrangement (RPA) (Cyber), you are reminded that you must also be able to evidence that relevant users have completed the free National Cyber Security Centre (NCSC) cyber security training for schools annually.

Policy templates such as the [Information Security Policy](#) and the [Acceptable Use Policy](#), are available via the [One West Members Area](#).

For further advice and guidance about the practical aspects of cyber, please contact our cyber leads at One West.



● Cyber Security in Schools: Key Lessons From the 2025/26 Survey

The Government's latest Cyber Security Breaches Survey highlights that cyber-attacks remain a significant and growing risk to schools. Almost half of primary schools (49%) and nearly three-quarters of secondary schools (73%) identified a cyber breach or attack in the previous 12 months. The increase is particularly notable for secondary schools, rising from 60% in 2024/25 to 73% in 2025/26.

What are the main risks?

Phishing remains the biggest threat. For those schools that experienced an attack or breach, phishing was reported by 90% of primary schools and 96% of secondary schools. This means a convincing email, message or login page remains one of the easiest ways for an attacker to gain access to a school's systems.

While schools generally have good technical protections, there are some areas where improvements could be made. They include:



- **Keeping systems up to date:** only 45% of primary schools and 62% of secondary schools met the survey's broader vulnerability-management measure, which includes having an appropriate patching policy alongside measures such as vulnerability testing or keeping anti-malware updated.
- **Supplier security:** this remains a particular weakness. Only 44% of primary and 48% of secondary schools met the survey's supply-chain security measure.
- **Staff awareness:** 72% of primary and 77% of secondary schools had provided cyber security training or awareness activities, leaving scope to ensure everyone receives regular training.
- **Personal data:** the survey found that 14% of primary and 18% of secondary schools held employee or pupil personal data that was not protected by measures such as encryption or anonymisation.
- **AI:** AI tools have already been adopted by 53% of both primary and secondary schools, but only 56% of relevant primary schools and 59% of relevant secondary schools had specific cyber security practices or processes in place to manage the associated risks.

Why does this matter?

A successful cyber incident is not simply an IT problem. A cyber incident can potentially disrupt access to school systems and files, compromise accounts and expose sensitive information. The survey found negative impacts on systems among 13% of primary schools and 20% of secondary schools that identified a breach or attack.

The report suggests schools therefore need to treat cyber security as part of their wider information governance, safeguarding, operational resilience, and business continuity arrangements, rather than leaving responsibility solely with IT.

ACTIONS TO TAKE NOW

Strengthen protection against phishing

Phishing is overwhelmingly the most commonly identified attack affecting schools. Provide regular, short cyber-awareness training for all staff, including temporary staff and volunteers. Make sure everyone knows how to recognise and report suspicious emails and unexpected requests for passwords, payments, or information.

Use multi-factor authentication and strong access controls

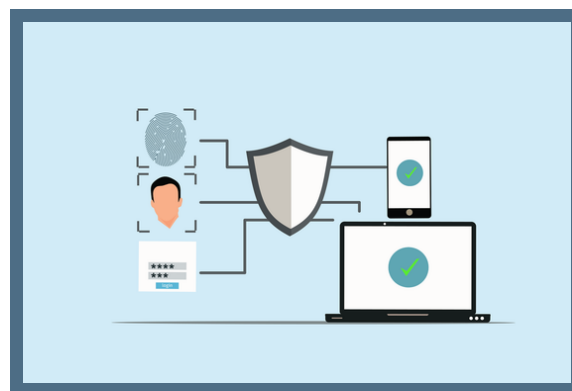
Check that multi-factor authentication is enabled wherever available, particularly for email, cloud services, and accounts with access to sensitive information. Adoption is already relatively high, with 89% of primary and 86% of secondary schools reporting two-factor authentication for networks or applications.

Patch systems promptly

Make sure operating systems, applications, devices and other software receive security updates promptly and that responsibility for checking updates is clearly assigned. Patch management remains an area where the survey identifies scope for improvement.

Protect your data backups

Review where pupil, parent, and staff information is stored, who can access it and whether appropriate encryption or other protections are in place. Maintain secure backups and ensure recovery arrangements actually work.



Check your suppliers

Don't assume that using a well-known provider automatically makes information secure. Schools should build cyber-security checks into procurement and periodically review suppliers that host, access, or process school information. The survey identifies supply-chain security as one of education's greatest relative weaknesses.

Be ready for an incident

Maintain an up-to-date cyber incident response and business continuity plan. Staff should know who to contact, how to escalate an incident, what systems are most critical, and when an incident needs to be reported externally. Although 73% of primary and 77% of secondary schools reported having formal incident-response plans, this still leaves a significant minority without one.

A key message for schools from this report is that cyber attacks are now a routine operational risk for schools, not a remote possibility. Governors and senior leaders should seek assurance that these controls are in place and regularly reviewed.

The full Government report, published on 30 April 2026, is available here: [Cyber Security Breaches Survey 2025/2026: education institutions findings](#)

● DPIAs: Start Early, Avoid the Last-Minute Rush

Many schools and organisations have experienced the same scenario: a new app, system, or service is ready to go live, the contract is about to be signed, and then someone asks, "Have we done a DPIA?" Unfortunately, by that stage, there is often little time to properly assess the risks.

A Data Protection Impact Assessment (DPIA) is not just an administrative exercise. It is a valuable risk assessment tool that helps schools and organisations identify and manage privacy, security, and safeguarding risks before personal data is used. This is particularly important when handling children's information.

Why should you care?

Even highly regarded tools can present unexpected risks.

They may:

- Transfer data outside the UK
- Collect more personal information than anticipated
- Use information for AI development or profiling
- Create safeguarding concerns
- Increase the likelihood of a data breach

A DPIA helps you to understand these risks and put appropriate controls in place before introducing a new system or process.

The biggest mistake: leaving it too late

A DPIA should be part of the planning process, not something completed after a decision has already been made.

Starting early means:

- Risks can be identified and addressed before contracts are signed



- Alternative solutions can be considered if concerns arise
- Staff are less likely to face unnecessary pressure or delays
- Schools and organisations can make informed decisions with confidence

In short, early DPIAs save time, reduce stress, and support better outcomes.

Who is responsible?

The school or organisation, as the data controller, is responsible for completing the DPIA. The project lead or service owner should coordinate input from the people who understand how the system will be used, including IT staff, safeguarding leads and operational or curriculum teams.

A common misconception is that the Data Protection Officer (DPO) completes the DPIA. In reality, the DPO's role is to provide independent advice, challenge assumptions where necessary, and offer assurance that risks have been properly considered.

A simple rule of thumb

Consider a DPIA whenever:

- Personal data is involved
- A new system, app, tool, or process is being introduced
- Existing uses of personal data are changing
- You are unsure whether there may be privacy or safeguarding implications

If in doubt, speak to your DPO as early as possible.

How we can help

We can provide you with a [DPIA template](#) incorporating screening questions, advice on whether a DPIA is required, support with risk assessments, and guidance on supplier assurances and contracts.

Remember: If a tool is worth using, it's worth checking. A short DPIA discussion at the start of a project can prevent issues later and help ensure that personal data is used safely, lawfully, and effectively.

● New Resources Available

Simplified DPIA Template

Our DPIA template has been refreshed, and now brings the screening questionnaire and full simplified DPIA into a single document.

You can view the new document here: [Simplified DPIA Template](#)

Freshly updated resources for Town Councils

Following a comprehensive summer review, we've refreshed our collection of Town Council-specific documents to ensure you have access to up-to-date resources.

From privacy notices and consent forms to model policies and SAR guidance, these templates are designed to save you time and can be tailored to meet your council's needs.

Explore the updated documents here: [Town Council Specific Documents](#)

New to the role of Headteacher or School Business Manager?

Starting a new role at the beginning of an academic year can be exciting, but it can also bring a host of new responsibilities.

To help you get started, we've put together a practical guidance document covering key data protection requirements and helping you prepare for your school's annual compliance review.

You can view the new document here: [Data Protection Essentials for New School Business Managers and Headteachers](#)

One of our DPO team members will contact you in the coming weeks to arrange the review. If you need any support before then, we're here to help so please do get in touch.

● Keeping Templates Up to Date

One West templates and guidance are reviewed and updated throughout the year as part of our continuous improvement approach.

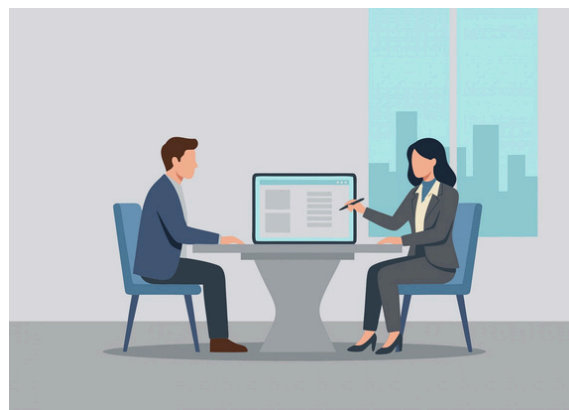
We therefore recommend that you download documents directly from the [Members' Area](#) whenever carrying out policy reviews, updates or compliance work.

The Members' Area should always be treated as the definitive source of current One West documentation, as locally saved copies may not reflect the latest version available. This helps ensure you are working from the most up-to-date templates, guidance and supporting resources at all times.

If you do not currently have access to the Members' Area, or would like a reminder of your login details, please contact us and we will be happy to assist.

● DPO Compliance Review Process for 2026/27

Following a review of our DPO Support Service, we have introduced a revised approach to Compliance Reviews and Support Calls for 2026/27.



Annual Compliance Reviews

Annual Compliance Reviews will remain the primary assurance activity for all clients.

Our updated review framework will provide:

- Greater focus on how data protection arrangements operate in practice.
- Enhanced preparation activities to help make best use of review time.
- Assurance on key areas from the recent update in legislation (Data Use and Access Act 2025)

Reviews will continue to be delivered either onsite or remotely, depending on local and service arrangements. They will also be making greater use of pre-review preparation and information gathering activities to ensure that time during the review is focused on your organisation's arrangements, priorities and opportunities for improvement.

Support Calls

The previous model of three scheduled Support Calls each year is being replaced with a more flexible, client-led approach. Clients will be able to access optional Support Calls between annual reviews to:

- Discuss progress against previous recommendations.
- Seek advice on emerging issues.
- Review new systems, suppliers or projects.
- Access additional support when required.

Continuing Support

These changes are designed to provide more focused assurance, greater flexibility and improved value from review activities, while ensuring ongoing access to advice and guidance throughout the year.

Members of the DPO team will be in touch over the coming months to arrange upcoming Compliance Reviews and provide details on accessing optional Support Calls.

● Stay Connected

DPPC 2026: Registration is Open!

The ICO's free virtual Data Protection Practitioners' Conference (DPPC) is taking place on **Tuesday 13 October 2026**.

We think this annual event provides an excellent opportunity to hear directly from the regulator on a range of current data protection topics, learn about emerging issues and regulatory developments, and take part in discussions with data protection professionals from across the sector.

You can view this year's programme of seminars here: [Seminars](#)

If you would like to attend, you can register here: [Register](#)

Follow us on LinkedIn

Over on LinkedIn we are sharing updates, practical guidance tailored to support your work, and creating a place for professional discussion and connection.

Whether you're looking to strengthen your processes or stay informed on best practices, our LinkedIn page will be an additional useful resource.

Follow us on LinkedIn: [One West | LinkedIn](#)

Thank you for reading

Warm wishes from all in the One West team!

