DPO NEWSLETTER

In this issue

You may notice our newsletter has a new look! We hope that you find this issue useful, and please remember that we are always here to help should you want to discuss any data protection matters with us:

I-west@bathnes.gov.uk 01225 395 959

Photos of Children Online - UKSIC Guidance

Recent guidance published by the UK Safer Internet Centre (UKSIC) has made a number of recommendations regarding the safe use of photography in schools. It is important to note that at present this is not a statutory obligation; the Information Commissioner's Office (ICO) and Department for Education (DfE) have not issued any changes to their guidance.

UKSIC's Key Recommendations:

- Ensuring images do not contain identifiable information that could be used to harm or blackmail an individual (e.g. full names or faces).
- Using imagery that is harder to misuse or abuse, this could be by only sharing photos taken from a distance, blurred images or images taken from over the shoulder.
- Applying privacy settings to help limit who can view and share content (this can be done on social media or any other place the images are stored or shared).
- Removing metadata (e.g. EXIF data) from the images that may reveal location, device details or timestamps. Such data can unintentionally reveal schedules or routines, for example of regular training.
- Embedding image security awareness and practices in staff training and policies.

As a data controller you should consider whether the UKSIC recommendations should be adopted or not, we advise that the second to fourth points should already be a part of your data protection practice as they form part of existing photography guidance.

The first point may be adopted as a precaution but as consent is sought from parents and privacy information is provided, the risk of the misuse or abuse of images and the potential vulnerability to blackmail should be understood by parents already. The risk is currently considered very remote but you may see some increase in the refusal to provide consent or the withdrawal of consent from parents, and you should be prepared to remove images if this occurs.

We will continue to update you on this topic but you may wish to review the full guidance in the meantime which can be accessed here: Protecting your setting's images from AI manipulation and abuse

Existing DfE and ICO guidance can also be found here:
Taking and using photos and videos, and using CCTV in schools (DfE)

Taking photos in schools (ICO)

Data Protection Complaints

On **19 June 2026** the new legal requirements regarding data protection complaints (within the Data Use and Access Act 2025) come into force.

The new law means organisations must:

1. give people a clear way to raise a data protection complaint;
2. acknowledge it within 30 days of receipt;
3. without undue delay, take appropriate steps to investigate and keep people informed; and
4. tell the complainant of the outcome.

If you have adopted our latest Data Protection Policy template, then all the above points are covered from a policy perspective, and you will need to ensure you follow this for any data protection complaints. We would recommend you reference the Data Protection Policy (for data protection related complaints) in your Complaints Policy.

We would also recommend you develop an eForm in order to provide people with a clear way to raise a data protection complaint. This could be an MS form/Google form or MS Word form which you can send out or publish on your website.

Annual Governance and Accountability Return (AGAR) - Assertion 10

From the 2025/26 AGAR, parish and town councils will be required to complete a new Assertion 10 as part of its Annual Governance Statement. The Assertion requires town and parish councils:

1. **Official Domain & Email** – to use an authority-owned domain (e.g., .gov.uk or .org.uk) for its website and generic staff/councillor email accounts. Personal domains like Gmail or Outlook are no longer permitted.

2. **Website Accessibility** – websites must meet WCAG 2.2 AA accessibility standards and have an up-to-date accessibility statement.
3. **Mandatory Policies** – must adopt and maintain up-to-date IT Policies and Data Protection Policies.
4. **Data Protection Compliance** – must be able to demonstrate lawful, safe handling of personal data, which includes regular data audits and staff/councillor data protection training.
5. **Transparency** - Compliance with the Freedom of Information Act (FOIA) and publication schemes, along with strict adherence to the Local Government Transparency Code.

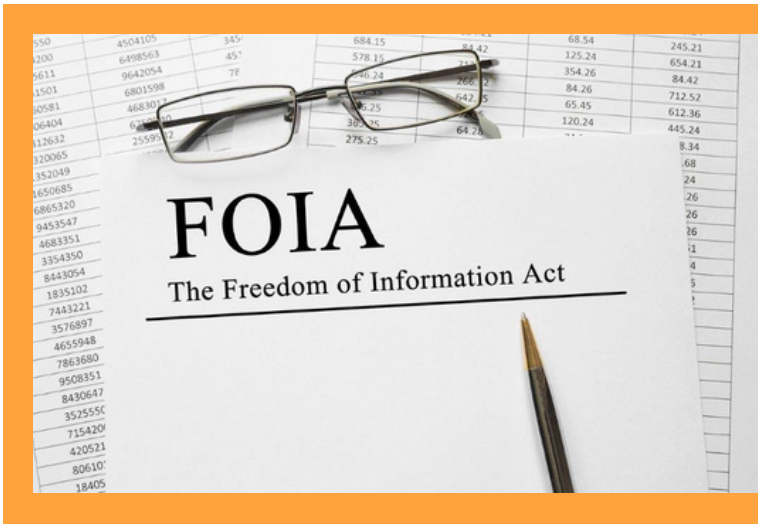
Please don't panic! As a DPO client we will support you with points 3 to 5 above, and your IT provider should be able to support you with points 1 and 2.

AI Generated FOIs - ICO Guidance

You may have noticed that requesters have started using AI to draft their Freedom of Information (FOI) requests, as well as their internal review requests if they are unhappy with an outcome. This is becoming much more common and often leads to less specific and broader requests.

It is important to remember that you can stop the clock and clarify requests with the requester so you can be sure that you are looking for the information they are interested in. If the request remains too broad and it will take over 18 hours of staff time to gather the information, you can apply the exemption set out in Section 12 (the cost of compliance exceeds the appropriate limit) of the FOIA 2000, and refuse the request.

The ICO has published some useful guidance on the impact AI has on FOI requests and how public authorities can handle them:
Freedom of Information (FOI) and Artificial Intelligence



Recent FOI Request - Incidents Related to Extremist Ideology

We have received multiple reports from schools about an FOI request which was received at the start of May, regarding incidents related to extremist ideology. The request sought information which had the potential to identify individuals and was broad in its definition of the "type" of incident.

Many schools noted that they don't record the type of incident in the way the requester had suggested and this caused some confusion. In instances where you aren't sure what the requester is seeking, or you need further clarification, you can stop the clock and seek this from them.

The request also asked specifically for information relating to 'schools under your trust'. Trust central teams are FOI bodies in their own right which would make any schools response to the extremist request "information not held". In the response the requester should be advised to direct their request to the central team.

It is good practice to consider who the request is addressed to as this will change who should be responding. This also takes the burden away from all individual schools within the trust as one central response can be sent.

Summer Holidays and SARs

With the summer holidays around the corner, this is a good time for all organisations to take a moment to plan ahead for any incoming Subject Access Requests (SARs) over the summer period. Whilst key staff may be away, the statutory obligations under the UK GDPR and Data Protection Act 2018 remain firmly in place. If you receive a new request during this time, you must still respond without undue delay and within one calendar month of receipt.

Remember:
The statutory timeframe starts when the SAR is received - not when it is read. However, if you need to undertake identity and/or authority verification, the one-month period only begins once you have received sufficient information to proceed.

If you request clarification, this will pause the clock, and it will restart once you have the requesters response. You should request any information you require without undue delay so as not to unreasonably hold up the request.

For SARs which are complex, you may be justified to apply a complexity extension which provides you with an additional two calendar months to respond. You can always get in touch with us so that we can help you review the level of complexity.

We would recommend that you consider the following steps to be prepared and remain compliant:

- Ensure you have a clear recorded SAR process in place (you may wish to use our latest SAR Guidance).
- Be clear on who is responsible for handling incoming requests, and plan cover as necessary.
- Ensure that access to records is maintained (this may need to be done remotely).
- Keep monitoring communication channels.
- If necessary, provide training for staff that may need to provide cover.

DPO Compliance Visits - What to Expect and How to Prepare

What will your compliance visit look like next academic year?

We will continue to use a combination of support calls and onsite visits to ensure schools receive the most appropriate level of support.

We recognise that arrangements for compliance visits may vary across schools and trusts, and in some cases may already be agreed. While compliance scores will continue to inform our approach, the format of visits may differ depending on each organisation's context and needs.

This may include a mix of support calls, onsite visits and remote DPO visits, as well as other approaches where appropriate. Our aim is to take a flexible and proportionate approach, ensuring that how we assess compliance is aligned to what works best for each school or trust.

Over the coming weeks, we will be in touch with schools and trusts to agree arrangements for the 2026 to 2027 academic year, ensuring the approach continues to support you effectively.

Easy tips to prepare for your DPO compliance activity

The start of Term 1 is a good opportunity to review your data protection arrangements and prepare for upcoming compliance activity. The One West team will notify you when updated policies, privacy notices and guidance documents are released. As most policies were updated in September 2025, you may wish to keep an eye out for any new versions over the coming months and ensure you are using the most up to date documents.

Whether this takes the form of support calls, onsite or remote visits, these tips will help ensure you are well prepared.

Inset days at the start of the academic year are a great opportunity for your staff to complete their annual data protection training and to share best practice. You can use the resources in our members area, or feel free to get in touch if you'd like us to run a session for you.

Reviewing your policies
Once you have identified any changes, you should consider whether your school policies and other guidance documents need to be updated. Where updates are made, ensure these are approved, uploaded to your website where required, and shared with staff and parents as appropriate. Getting policies reviewed and approved at the start of the academic year can help ensure you are confident in your compliance. Where material changes are made, it may be helpful to ensure staff are aware and understand any updates.

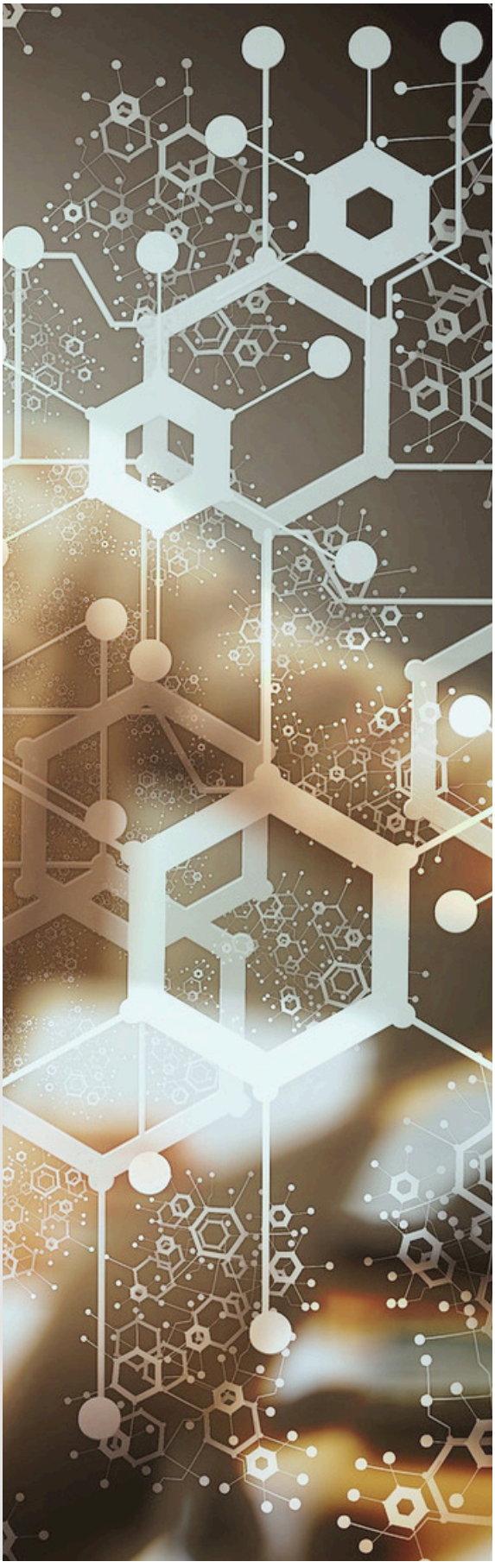
Consents
This is also a good time to remind parents and staff that they can review and update their consent preferences if required.

Systems and DPIAs
At the beginning of the academic year, there are often changes to contracts, systems or suppliers. This is a useful opportunity to review your Data Protection Impact Assessments (DPIAs) and make sure they reflect any changes in how you are processing data. We are happy to support you with this and can review any updates.

Your RoPA
Once this has been completed, ensure that your Record of Processing Activities (RoPA) is reviewed and updated as needed so that it remains accurate and up to date.

How things work in practice
It can also be helpful to consider how data protection works in practice across the school. The DPO walkaround checklist can be a useful tool to sense check how personal data is handled day to day.

Finally, please don't view our compliance activity as inspections. They are designed to support you, and our dedicated team is available to provide guidance and advice whenever required.



Thank you for reading

As summer begins, we hope you find time to rest, recharge, and enjoy the season. Warm wishes from all in the One West team.

One West