Information Commissioner's Office

Edtech examined

Key findings from our audits

ico.
Information Commissioner's Office

Foreword

Protecting children's privacy is a top priority for the ICO. Through our children's code strategy, we've pushed social media and video-sharing platforms to change their practices, driving real change for millions of young users. But the classroom is different. Children don't choose which education technology (edtech) products their school uses, and they may not be able to opt out. That's why schools, parents, and children should be able to trust that the digital tools used in the classroom are safe and meet the highest data protection standards.

Behind every school login screen, every homework app, and every register, a system is collecting children's personal information. This ecosystem of edtech that supports teaching and admin in UK schools is vast and deeply embedded in everyday learning. Schools, edtech providers, and sub-processors form a web of relationships, so it isn't always clear who is responsible for the children's information they collect or use.

During 2024 and 2025, we carried out consensual audits with 28 edtech providers whose products are widely used across primary and secondary schools. We looked at:

- management information systems;
- safeguarding tools;
- behaviour management platforms;
- learning management systems;
- classroom apps; and
- data integration services.

We found much to encourage us, particularly about information security. But we also found compliance gaps. Many providers didn't always correctly identify whether they were processors or controllers, especially when they used children's information for product development or analytics.

Other common issues included:

- insufficiently detailed contracts with schools;
- incomplete data flow mapping;
- weak application of data minimisation and storage limitation principles;
- outdated or inaccessible privacy information; and
- gaps in data protection impact assessments.

In total, we made 596 recommendations, and providers accepted almost all of them.

The findings from these audits will give us a broader understanding of data protection risks and practices in the UK edtech sector. The UK government has its own priorities for the education sector. We are engaging with them on secondary legislation that will require us to provide a new code on the use of children's personal information in digital systems in educational settings. The findings from this work will help inform the development of that code.

Katie Searle
Director of Children's Strategy

Contents

Introduction

What is edtech?

The Department for Education has described edtech – or education technology – as "the practice of using technology to support teaching and the effective day-to-day management of education institutions". Edtech describes products used in schools and other education institutions or at home.

UK data protection law does not define Edtech, and we haven't tried to create a definition while completing these audits. Where we refer to edtech in this report, we have adopted the language used by schools and the wider sector.

Where we refer to edtech providers, we mean the organisations selling or providing – and often developing – technology products and services used by schools. UK data protection law applies to all organisations in the UK or that process the personal information of citizens in the UK. This includes edtech providers using children's information on behalf of schools or for their own purposes.

Where we refer to schools, we mean educational settings delivering primary or secondary education, or both. This includes:

- community or local authority maintained schools;
- foundation or voluntary schools;
- faith schools;
- independent schools; and
- academies or academy trusts.

Where we refer to schools in this report, we mean the different types of schools in England, which are usually the controllers when processing children's personal information. However, our findings may also be relevant:

- to schools and local authorities in Scotland, Wales and Northern Ireland; and
- when multi-academy trusts or local authorities are controllers instead of schools.

How is edtech used in practice?

Schools typically use a **management information system** to store and manage all pupil information. Management information systems are a school's primary database and store the largest amount of children's personal information, including:

- name and date of birth;
- contact information, including home address;
- contact details for family members; and
- sensitive information such as:
    - ethnicity;
    - pupil premium status;
    - health information; and
    - special educational needs and disabilities.

Schools use a **safeguarding system** to log and report pupil safeguarding incidents and the actions taken. Larger schools – especially secondary schools – also use a **behaviour management system** to track and influence pupil behaviour. Safeguarding and behaviour management systems collect more children's information in logs of incidents, particularly about safeguarding or behaviour events involving the child.

Secondary schools often use a **learning management system** to assign and manage online learning content and homework. These systems typically process at least the following information:

- the child's name;
- their class or age group;
- their school; and
- their usage and learning progress information.

Learning management systems also often collect more sensitive information to support school reporting of learning progress and trend analysis, including:

- gender;
- ethnicity;
- pupil premium status; and
- special educational needs and disabilities.

Schools use a range of **classroom learning apps** to provide learning resources and activities, especially in core national curriculum subjects such as Maths and English. There is often a classroom learning app for each age group and subject. Children progress to a different learning app as they move through the school curriculum.

Some of these collect no children's personal information. However, the majority use:

- the child's name;
- their class or age group;
- their school;
- their usage and learning progress information; and

- demographic information such as:
    - gender;
    - ethnicity;
    - pupil premium status; and
    - special educational needs and disabilities.

Several classroom learning apps are also available for children to use at home on their own devices.

Most schools use a **data integration service** to:

- share pupil information from the management information system with other edtech products; and
- manage the flow of personal information between different edtech products.

Integrations typically require school approval before activation, such as from a senior school leader or the IT team. Alternatively, a member of school staff can manually upload pupils' personal information to many edtech products.

How did we review edtech?

In 2024 and 2025, our Regulatory Assurance team completed a programme of consensual audits looking at edtech. We completed audits with organisations we identified as providing edtech products or services used in the classrooms of:

- primary schools (children aged 4-11 years); and
- secondary schools (children aged 11-17 years).

We wrote to edtech providers, inviting them to work with us and support our work. We explained that our goal was to understand:

- how their products handle children's personal information; and
- how they have mitigated privacy risks and complied with UK data protection law.

We explained that these audits were voluntary, and we didn't exercise our formal powers.

Edtech providers worked positively with us, and we worked with 28 providers covering numerous edtech products used by schools.

In completing audits, we followed our data protection audit methodology and framework. Audits involved:

- technical demonstrations of edtech products;
- a review of publicly available information;

- face-to-face discussions or written correspondence; and
- a review of supporting documents, including:
    - privacy notices;
    - Data protection impact assessments (DPIAs);
    - records of processing;
    - written contracts with schools;
    - internal policies and staff training; and
    - other evidence of compliance.

We initially identified edtech providers through open-source research, web searches, and information from around 500 schools. We narrowed this down by reviewing the websites and privacy notices of edtech providers. We prioritised having a variety of different edtech products and types, education stages, and provider organisation types. Our aim was to collect a representative sample of the different types of edtech products used in classrooms.

The edtech products we reviewed

In selecting edtech providers to engage with, we focused on a number of key categories:

- **Curriculum and learning apps** that provide learning resources and activities. This is a dynamic market with a vast number of products available. We worked with a large range of different products, from some of the most commonly used apps in classrooms to new startup products.
- **Learning management systems** that assign and manage online learning content and homework. We estimate that over 70%* of UK schools use the providers we worked with.
- **Behaviour management systems** that track and reward pupil behaviour. We estimate that over 70%* of UK schools use the providers we worked with.
- **Safeguarding systems** that log and report safeguarding incidents and actions taken. We estimate that over 90%* of UK schools use the providers we worked with.
- **Management information systems** that store and manage all pupil information. We estimate that over 85%* of UK schools use the providers we worked with.
- **Data integration services** that share pupil information between edtech products. We estimate that over 90%* of UK schools use the providers we worked with.

* These percentages are estimates based on the approximate numbers of schools using each edtech product we reviewed, where providers shared this information with us.

While our work covered a range of edtech products used in school classrooms, we didn't work with:

- providers of school servers or IT networks;
- online environments or workspaces;
- video-conferencing products;
- generative AI chatbots or assistants;
- systems designed to monitor children at school, such as device-monitoring tools such as keystroke or web-filtering solutions;
- physical monitoring solutions, such as CCTV, facial-recognition technologies, or smart bathroom sensors; or
- edtech products or information society services that are only used at home, as we cover these in our children's code strategy.

We took our findings as a snapshot in time as of each audit.

As the audits started before the Data (Use and Access) Act 2025, our findings do not address changes made by the act, such as children's higher protection matters introduced to UK GDPR article 25.

We haven't identified specific organisations or edtech products in this report, as we intend our findings to benefit and inform the whole sector. Each organisation received an individual audit report that identified specific opportunities and recommendations to improve compliance and processes. Case studies are based on real audit findings but have been de-identified.

We have described potential harms generally based on our data protection harms research and taxonomy, as we didn't receive evidence of actual harm to children.

What happened after each audit?

Every edtech provider received detailed findings and specific recommendations for improving its data protection compliance. In total we made:

- **596 recommendations**, 98% of which edtech providers accepted and put actions in place;
- **139 advisory notes** offering general observations and advice; and
- **118 good practice notes** where providers had taken clear positive measures to protect children's information.

After each audit, we also asked edtech providers for feedback on their experience and the value added:

- **76%** felt that engaging with us helped them mitigate data protection and privacy risks in their products.

- **75%** felt we helped them further understand the requirements in UK data protection law.
- **83%** felt the audit helped raise awareness of the importance of protecting children's information across their organisation.

We continued to work with 12 of the 28 edtech providers after the audits. We requested that they provide further information to demonstrate how they are improving their data protection compliance. We are reviewing progress and supporting evidence in key risk areas to confirm that providers have completed the agreed actions.

Key findings

Our key findings were:

1. Identifying the controller for each processing activity

We found that edtech providers hadn't always correctly determined their role as a controller or processor for each processing activity in their product.

Most of the edtech providers we engaged with determined they were processors of children's personal information and were acting only on the school's instructions. However many providers also used children's information for their own additional purposes – such as developing products or producing anonymised information – without recognising that they were controllers of this additional processing.

When providers didn't identify themselves as controllers of specific processing activities, they usually hadn't met the responsibilities of controllers in UK data protection law. This resulted in gaps in safeguards to protect children's privacy.

2. Using personal information for other purposes

We found that edtech providers need to assess whether reusing children's information for their own purposes complies with the law, before they do so.

Many edtech providers – especially those offering classroom learning apps – used children's information to:

- analyse product performance;
- develop and test new products; and
- produce anonymised information for other purposes.

Some also used children's information to train AI functionality or shared anonymised information with third parties. One provider had previously used children's information to create anonymised pupil profiles to sell to third parties conducting education research.

Providers often couldn't demonstrate that this additional processing was fair, as they only had access to children's information because of their role as a processor. They hadn't always identified a lawful basis for the further processing. Using children's information in a way that isn't fair or has no lawful basis is a breach of UK data protection law and can lead to children losing control of their information.

3. Having detailed contracts and terms

We found that contracts between edtech providers and schools need to:

- explain the proposed processing of children's information in more detail; and
- give providers clearer, more comprehensive processing instructions to follow.

When we reviewed written contracts and processing instructions, many didn't describe clearly how providers would use children's information. Broad or vague terms or unclear instructions led providers to make their own decisions and determine the purposes and means of processing for themselves. Where contracts lacked sufficient detail, several providers also used children's information for their own purposes, and couldn't show that schools had instructed them to do so.

Unclear contracts also make it difficult for schools to fully understand how their pupils' information was being used. This can significantly affect their wider data protection compliance and could contribute to a lack of autonomy for schools as controllers.

4. Mapping and recording processing activities

We found that providers need to:

- more fully map all data flows into, through and out of edtech products; and
- keep complete records of their processing activities.

Almost every edtech provider had incomplete or insufficiently detailed records of processing activities, or they hadn't fully mapped all of the data flows relating to their product. We noted several types of missing information, such as:

- technical and organisational measures to secure children's information;
- records of any transfers of information internationally to sub-processors; and
- logs of any additional use of children's information for the provider's own purposes.

Where records of processing activities were inadequate, this often contributed to gaps in data protection oversight, or a general lack of staff awareness of how children's information is used.

5. Explaining the use of children's personal information transparently

We found that information and resources explaining how children's personal information is used need to be more detailed, and made available so schools, families and children can make informed decisions about the privacy risks.

While most edtech providers published a privacy policy on their website, these often only gave general information about their product and how they used children's information in practice. Many privacy policies also had missing or unspecific information. Several hadn't been regularly reviewed and included inaccurate, outdated information.

Positively, some edtech providers – especially smaller organisations – made detailed resources, privacy explainers, and evidence of their safeguards available proactively on their website or in dedicated online portals. However others couldn't show how their use of children's personal information was transparent to schools. This may make it difficult for schools to inform families and children about how edtech products use their information, which could reduce trust in edtech use.

6. Retaining information for only as long as necessary

We found that edtech providers need to set out their retention periods and explain:

- how they will assess how long they need to keep children's information; and
- how they will delete the information.

Many edtech providers hadn't set or recorded specific retention periods for children's information clearly enough in their privacy information, records of processing activities, or retention schedules. In some cases, providers couldn't justify why they were keeping children's information, which meant they kept it longer than necessary and therefore held excessive information.

In several cases – especially for providers of classroom learning apps – it wasn't clear what action the provider would take at the end of the retention period (ie whether they would anonymise or delete information). In practice, they often anonymised information instead of deleting it. In an isolated instance, information labelled as 'anonymised' was still identifiable, and providers were keeping it indefinitely.

Where providers keep children's information for longer than needed, this:

- significantly increases the risk of a personal data breach or misuse of the child's personal information; and
- breaches the storage limitation principle in article 5(1)(e).

7. Doing a data protection impact assessment (DPIA)

We found that providers didn't always complete DPIAs when required. They didn't assess or describe in enough detail how they used children's information or what safeguards were in place to protect children. Edtech providers need to carefully assess the risks to children when using their information and manage those risks more robustly.

The DPIAs we reviewed were often not detailed enough or were missing details about the product, use of the information, and safeguards in place.

Many edtech providers hadn't fully assessed the potential risks to children and their privacy when using their information, or they had only assessed the potential risks to themselves rather than to the child. Several DPIAs also didn't include:

- advice from the data protection officer (DPO) or lead;
- outcomes of meaningful consultations with key stakeholders; or
- senior leadership sign-off.

In many cases edtech providers hadn't done a DPIA at all where one was required. Usually this was because the edtech provider had incorrectly determined they were a processor when they were a controller in practice. Where DPIAs hadn't been done or weren't detailed enough, there were typically also gaps in safeguards or the wider data protection approach.

8. Overseeing sub-processors

We found that edtech providers need greater control and oversight of their sub-processors. They must ensure due diligence checks and school authorisation are in place before granting access to children's information.

Not all edtech providers had obtained written authorisation from the appropriate school leader, undertaken due diligence checks, or fully reviewed contractual terms before giving sub-processors access to children's information. Where they sought authorisation, providers typically relied on general authorisation clauses in written contracts rather than obtaining specific authorisation for each new sub-processor. On a few occasions, providers had used sub-processors with problematic contractual terms that they only became aware of during our

audits, such as sub-processors stating they would keep a copy of children's information to train their AI.

Around half of the edtech providers we engaged with also hadn't regularly checked that their sub-processors were maintaining the agreed safeguards and using children's information as agreed in the contract. This was more common among larger providers offering management information or safeguarding systems and suites of classroom learning products, as they typically used more sub-processors.

9. Handling personal data breaches

We found that personal data breach processes need to clearly set out how edtech providers will:

- identify and investigate breaches; and
- report them quickly to us, schools, and affected people.

Most edtech providers had documented their personal data breach processes in policies available to staff. However these were usually too broad and didn't set out key stages, such as:

- how providers would decide whether to report breaches to us or notify affected people;
- when they would make those decisions; and
- who would be responsible for such decisions.

Providers were often unclear about their responsibilities as controllers or processors, particularly the requirement as processors to report all breaches – regardless of the risk level – to schools without undue delay.

Several edtech providers had never logged a personal data breach or near miss. They had no assurance that staff were following reporting processes or that those processes worked in practice. When a provider logs no incidents and doesn't regularly test breach identification processes, there is a risk that breaches are happening but going undetected and unresolved.

10.Taking a data protection by design approach

We found that edtech providers need a robust internal framework for product design and development, which puts the protection of children's information and their privacy at the heart of every decision.

Several edtech providers – especially those offering safeguarding systems – had taken steps to protect children's information in their products. They had:

- designed products to be highly configurable by schools;
- turned off all non-core functionality and processing by default; and
- implemented robust multi-level access management and user authentication.

However, not all edtech providers could demonstrate that they had prioritised data protection in their product development. Examples included cases where providers had:

- rolled out new product features with them switched 'on' by default;
- built products with back-end areas where personal information couldn't be erased or retrieved, including for individual rights requests; or
- introduced AI functionality without adequate safeguards.

Some edtech providers had also failed to set clear internal policies or provide sufficient training or guidance to staff about protecting children's information.

Detailed findings and case studies

Controllers, processors, and lawfulness

At a glance:

- We reviewed whether edtech providers had correctly determined their role as a controller or processor and were fulfilling their responsibilities. We checked whether providers had identified appropriate article 6 lawful bases and article 9 conditions when they were the controller.
- We found that most edtech providers had determined they were processors of children's personal information. However, many also used children's information for their own additional purposes but hadn't recognised that they were controllers for this processing. As a result, they weren't fulfilling their responsibilities.
- We told edtech providers to review each individual processing activity and determine whether they were processing children's information:
    - under the school's explicit written instructions (as a processor); or
    - for their own purposes (as a controller).

  As providers are controllers for any additional use of children's personal information for their own purposes – such as developing products or producing anonymised information – they must:
    - identify an article 6 lawful basis and article 9 condition; and
    - ensure all additional processing complies with data protection law.

Findings

Controller or processor

The UK General Data Protection Regulation (UK GDPR) defines the controller as the person or organisation that:

> "determines the purposes and means of the processing of personal data".

Edtech providers will be controllers when they exercise overall control of the personal information they process. When providers are the controllers, they are responsible for ensuring their processing complies with UK data protection law. They must be able to demonstrate compliance with the data protection principles.

UK GDPR defines a processor as a person or organisation that:

> "processes personal data on behalf of the controller".

Edtech providers will be processors when they process personal information only on behalf of their school clients. This must be governed by a binding written contract or other legal act with each school that sets out:

- what they use children's personal information for; and
- how they process it.

Providers must only process information on each school's documented instructions.

When an edtech provider determines the purposes and means of processing, they are the controller as in UK GDPR article 28(10). This means that the provider – not the school – is responsible for complying with UK data protection law. For example, an edtech provider is a controller – not a processor – if they use children's personal information beyond or outside of the written contract with schools or the documented instructions from schools. This is because the provider is determining the purpose and means of the processing.

The vast majority of edtech providers we engaged with had determined they were processors and were acting on the school's instructions, with the school as the controller. We agreed that they were processors when using children's personal information in order to provide the core edtech product and service, following the written contract and documented instructions.

However, almost 70% of providers were found to be the controller for some of their uses of children's personal information, but they:

- hadn't recognised this; and
- weren't fulfilling their responsibilities as controllers.

We often found edtech providers were actually controllers when they were:

- using children's information beyond the instructions set by the school – or not as instructed – in the written contract or processing instructions from the school;
- making significant decisions themselves about the means and purpose of processing when providing the core edtech product and service;
- using children's information for their own additional purposes, such as developing products or product features or training AI functionality; and
- anonymising children's information for their own purposes.

Organisations can be processors and controllers when they process the same personal information for different purposes. We found this was common for edtech providers, especially when they repurposed children's information for their own purposes.

When we found edtech providers were controllers in practice and hadn't identified this, we also often found that written contracts either weren't in place or were too broad and unspecific. This led to unclear or undocumented processing instructions from schools, which meant edtech providers determining the means and purposes of processing themselves.

We told edtech providers to use the checklists in our Guide to controllers and processors to help determine if they are a controller or processor. If you determine the purposes and means of processing, you are a controller, regardless of how any contract about processing services describes your role.

Lawful basis

When edtech providers were controllers using information for their own purposes, they hadn't always identified a valid and appropriate article 6 lawful basis. They also hadn't always identified an article 9 condition when using special category data.

Some providers told us they relied on legitimate interests. However, they hadn't completed a legitimate interests assessment to balance their own interests with those of children and their families. They often hadn't recorded lawful bases and article 9 conditions clearly and consistently in the:

- record of processing activities (ROPA);
- privacy information;
- DPIAs; and
- other relevant documents.

We told edtech providers to review our guidance on what do we need to consider when choosing a basis for processing children's personal data, especially before relying on a child's consent (or a parent's consent for children under 13 years), or a contract with a child, as a lawful basis for using the child's personal information.

Outcomes

The edtech providers we engaged with agreed to:

- review their role as a controller or processor; and
- fulfil the relevant responsibilities.

Edtech providers that we followed up with have taken steps to:

- determine their role as a controller or processor correctly; and

- ensure they fulfil their role effectively for each processing activity (eg by updating written contracts with schools).

Case studies

Case study: An edtech provider told us they were:

- a processor when using children's information to provide the edtech product; and
- a controller for additional uses, such as monitoring product performance and developing new features.

Their ROPA didn't clearly record their role for each processing activity, and the provider had stated their role unclearly and inconsistently across several internal documents. They had a written contract with schools; however, it was generalised and didn't record specific terms or processing instructions. It also described them as a controller and a processor interchangeably without context or explanation, which was confusing and risked misleading schools.

The provider had misunderstood the lawful bases in UK GDPR article 6(1) and relied on both (b) contract and (f) legitimate interests for additional processing for their own uses. However, they didn't have a contract with children as the data subjects. They also hadn't balanced their own legitimate interests with the interests, rights, and freedoms of the children. Their additional use of children's personal information involved special category data, including children's ethnicity and health information, but they hadn't identified an article 9 condition.

We told them to:

- update their ROPA, written contract with schools and internal documentation to ensure that they record their role as a controller and processor correctly; and
- clearly record a valid article 6 lawful basis and article 9 condition for additional processing when they are a controller.

Over the following six months, they:

- completed a detailed legitimate interests assessment, balancing their own interests with the children's interests;
- removed references to relying on contract as a lawful basis;
- updated their ROPA and written contract, making them much clearer; and
- prepared revised contracts to roll out to schools at renewal.

Case study: An edtech provider told us they were a processor only; however, in practice, they were a controller.

When using children's information to provide the edtech product and service, they decided on the means and purpose of processing. They set universal retention periods in their product with no option for schools to change them. They also released updates and launched new product features and new uses of children's personal information by default, with no option for schools to turn them off. They had basic terms of use but didn't have a written contract, data processing agreement, or other written instructions with schools.

They also repurposed children's information to produce anonymous information for analysis. They used children's information from all schools to develop their single central product. With incomplete data flow maps, no mention of these processing activities in privacy information and no written contract, schools were unlikely to know their pupils' personal information was used in this way or to be able to control it.

We told them to:

- map how they used children's personal information fully;
- identify whether they were the controller or processor for each use; and
- either give schools control or meet their responsibilities as controller.

We followed up with them in the following six months. They had:

- engaged an external DPO service to map their processing activities;
- begun rolling out configuration options in their product to give schools control of the processing;
- added explanations of additional uses of children's information to their privacy information; and
- begun updating their written contract with schools with specific instructions they will follow.

Case study: An edtech provider told us they were an independent controller with each school for the use of children's information in their product.

In practice, schools and the provider shared decisions about processing. Schools determined what information to give to the provider. The provider:

- determined the data fields required for each specific processing activity;
- decided how they processed the information; and
- managed retention and data sharing.

Both the school and provider could edit and delete children's personal information from the product.

The written contract stated that both parties were independent controllers, but it didn't clearly explain how the provider and the school would:

- split controller responsibilities; or
- handle individual rights requests or personal data breaches.

In practice, the provider directed individual rights requests they received back to the school, despite being responsible for handling those requests themselves as a controller.

We told them to:

- carefully review their role and their use of children's personal information; and
- clearly record how each controller would meet their data protection responsibilities.

When we followed up with them, they had reviewed their role as a controller and begun taking steps to ensure they fulfilled their responsibilities. This included plans to:

- amend written contracts with clear processing instructions; and
- set out how they would work with schools to respond to individual rights requests from children and manage personal data breaches.

These changes will help to ensure the provider and schools are clearer about their data protection responsibilities. We are continuing to work with the provider to ensure they fulfil their responsibilities as an independent controller.

Case study: An edtech provider had taken several steps to ensure they were a processor for all uses of children's personal information in their product.

They designed their product to be highly configurable by schools with a wide range of settings available. From a configuration dashboard, schools had to decide:

- which data fields they collected;
- how they formatted information;
- how long they retained information; and
- other aspects of how they used the information.

All non-essential uses were off by default until the school activated them. The provider's internal policies strictly prohibited any repurposing of personal information. They carried out product development and debugging using only synthetic data for testing. Written contracts included detailed explanations of every possible use of children's information.

These measures ensured that schools meaningfully controlled how children's information was used in practice and made almost all decisions about its use.

Further reading – ICO guidance

- Controllers and processors
- Contracts and liabilities between controllers and processors
- Principle (a): Lawfulness, fairness and transparency
- Using children's information: a guide
- Children and the UK GDPR
- A guide to lawful basis
- What is valid consent

Data flows and records of processing activities

At a glance:

- We reviewed whether detailed information about processing activities and data flows into, through, and out of edtech products had been recorded in writing and kept updated.
- We found almost every edtech provider had incomplete or insufficiently detailed records of processing activities, or they hadn't comprehensively mapped all of the data flows relating to their product.
- We told edtech providers that they must have complete and accurate records of processing activities, including detailed information about their use of children's personal information and the safeguards in place to protect it.

Findings

Most organisations need to maintain a record of processing activities. Both controllers and processors need to:

- keep these records in writing or electronic form; and
- ensure they include the information required in UK GDPR article 30(1) for controllers and 30(2) for processors.

ROPAs are important because they help organisations understand how they:

- process personal information;
- monitor the flow and sharing of personal information; and
- identify and mitigate risks.

There is a limited exemption for organisations employing fewer than 250 staff, but only under certain circumstances. Most edtech providers we worked with – especially providers of classroom learning products – employed fewer than 250 staff. However, they used personal information regularly, and this often included special category data. Therefore, they still need to produce and maintain records of this processing.

Data flow mapping

Mapping the data flows into, through, and out of edtech products is vital to produce and maintain an accurate ROPA. The majority of edtech providers had done at least some information audits or mapping of the data flowing into and out of their product.

Some providers had produced extensive diagrams and charts showing data flows at a granular level.

For management information systems, school staff collected children's personal information during their admission to the school and entered it manually. For other edtech products – such as behaviour and safeguarding systems, learning management systems, and classroom learning tools – children's personal information usually entered the product through either:

- manual entry or upload by school staff; or
- automatic regular import from the school's management information system via a data integration service or application programming interface (API).

When edtech providers used a data integration service or API, they sent a request for the mandatory and optional data fields to share, which the school reviewed and authorised. Schools could enable or disable each optional field before authorising the request, but they couldn't change mandatory data fields. If they wanted to change these, they had to decline the request and ask the provider to resend it.

We told edtech providers to conduct data flow mapping or information audits regularly, to capture changes and ensure the ROPA is accurate and updated. Using automated tools or software, or manually checking access logs, can help providers identify any additional or secondary uses of personal information that they might have missed.

Records of processing activities

Almost 90% of edtech providers were missing required information about their use of children's personal information in their ROPA, or had an incomplete ROPA that didn't record all processing taking place.

Required information that was often missing included:

- transfers of personal information internationally and the safeguards in place;
- the technical and organisational security measures; and
- for controllers, the categories of data subjects and personal information, and retention periods – especially when the edtech provider hadn't identified that they were the controller and needed to record this additional information.

Incomplete ROPAs and unrecorded processing were often the result of providers not effectively mapping or regularly updating their data flows. We also often found that providers recorded the processing activities they carried out as processors but didn't record secondary uses or additional processing of children's information for their own purposes as controllers. Examples of unrecorded additional uses were:

- developing products or product features;
- testing whether new features worked with live information;
- training AI functionality and testing for accuracy, fairness and bias; and
- producing pseudonymised or anonymised information and pupil profiles.

Without a complete ROPA that captures all processing activities and includes the required information, edtech providers may not be fully aware of how they use children's information. As a result, they don't ensure safeguards are in place or mitigate potential risks to children. For schools as controllers, they may not fully understand how a provider uses pupils' information if they don't have enough technical information about the processing. This makes it very difficult for them to control use of the information or meet their own compliance responsibilities.

We suggested that edtech providers share their ROPA – or relevant extracts – with schools. Giving schools a full picture of how the provider processes children's personal information allows them to fulfil their own compliance responsibilities.

Outcomes

The edtech providers we engaged with agreed to:

- improve their ROPA where it didn't meet the required standard; and
- regularly map data flows into, through, and out of their edtech products.

The providers we followed up with have updated their ROPA to include all the required information and all processing of children's personal information.

Case studies

Case study: An edtech provider had created a high-level data flow map for the product and had produced a ROPA, but the ROPA was very basic. The provider recorded key processing activities that were essential to delivering the edtech product and service. However, the ROPA didn't include information about:

- technical and organisational security measures; or
- whether the provider would transfer information to third parties, including internationally.

The provider regularly repurposed children's information for their own purposes, including to develop their product and to produce pseudonymised pupil profiles, but they didn't record this in the ROPA. They also failed to record important information about this additional use, including the purpose, lawful basis, and retention periods, either in writing or electronically.

We told them to update their ROPA with this information and shared the ROPA templates available on our website. We followed up with them in the following 12 months and reviewed the improved ROPA, which was more comprehensive and included the information required in UK GDPR article 30.

Case study: An edtech provider completed data flow mapping exercises quarterly using a range of automated and manual tools and checks. They maintained a comprehensive ROPA. The ROPA included a complete inventory of the children's personal information held and how exactly they processed it. For each specific processing activity, the ROPA stated whether they were a controller or processor and included the information required by article 30. It also provided additional information such as:

- information sources and storage locations;
- justification for lawful bases and retention periods;
- links to DPIAs or entries in the organisation risk register;
- records of personal data breaches; and
- free text fields in the product, where users could input additional unnecessary personal information that the provider needed to delete regularly.

The ROPA was a living document that the DPO and senior leaders updated and reviewed regularly. As a result:

- staff had a good understanding and awareness of how children's personal information was being used in their product; and

- the provider had a strong organisational culture of handling children's information carefully.

Further reading – ICO guidance

- Records of processing activities
- Is there a ROPA template we can use?
- Data sharing

Data minimisation, purpose limitation, and storage limitation

At a glance:

- We reviewed how edtech providers processed children's personal information in edtech products and whether they:
  - limited collection to only what was necessary;
  - stored information only for as long as necessary; and
  - avoided using information for additional incompatible purposes.
- We found that edtech providers often failed to set specific retention periods for children's information or record them clearly. Many providers collected more information than needed or used children's information for their own purposes and couldn't show how these uses complied with the law.
- We told edtech providers to:
  - use and store children's information only for as long as necessary or as instructed by the school as controller;
  - review any additional use of children's personal information beyond the delivery of the contracted service; and
  - set out retention periods and erasure processes more clearly in privacy information and written contracts with schools.

Findings

The UK GDPR sets out seven data protection principles that are fundamental to processing personal information compliantly. Purpose limitation, data minimisation, and storage limitation are three of these principles, set out in UK GDPR articles 5(1)(b), (c), and (e) respectively.

When edtech providers are controllers, they must comply with these principles. This includes:

- using only the minimum personal information they need;

- using it only for specified purposes and not in ways that are incompatible with these purposes; and
- storing it for only as long as necessary to fulfil these purposes.

When edtech providers are processors, they should support schools by using their knowledge as developers and building their products with data protection principles in mind. Designing edtech products in this way makes it easier for schools to fulfil their compliance responsibilities, and may give providers a competitive advantage.

Using the minimum personal information

Management information systems are usually the school's main system for storing information. They collect and handle most of the personal information the school holds about each child. Providers of management information systems often let schools:

- tailor the type and amount of personal information collected; and
- collect additional information if they wish.

Other edtech products use only a subset of each child's record. Most of the products from the providers we worked with used at least the child's:

- first and last name;
- unique pupil number or admission number;
- school year or class registration groups;
- date of birth; and
- school email address (for edtech products used in secondary schools).

We found that almost 50% of providers hadn't fully considered data minimisation. They either collected unnecessary personal information that their product didn't need to function, or they couldn't demonstrate why some of the personal information collected was necessary. This was the case for most classroom learning product providers. As a result, they weren't limiting the personal information processed to only what was necessary. Most of these providers also used children's personal information for their own purposes and hadn't assessed or couldn't justify how these additional uses complied with the law.

Providers often collected additional personal information or special category data about each child to support school analysis of learning progress, including:

- gender;
- ethnicity;
- language and additional languages;
- health or medical conditions;

- special education needs and disabilities; and
- free school meals and pupil premium status.

Some providers made these optional fields and let schools decide whether to share this sensitive information. However, others made them mandatory, so they collected the information automatically if the school used the product.

We told edtech providers to:

- assess the minimum amount of children's personal information needed to operate each element or feature of the edtech product; and
- record this in product design specifications or in a DPIA.

For classroom learning products and learning management systems, we suggested these practical ways to adopt data minimisation:

- Use the child's initials, first name and initial, or a username or pseudonym by default, instead of the full name.
- Assign each child your own unique identifier, instead of their national unique pupil number or admission number.
- Use the child's school year or month and year of birth, instead of their full date of birth.
- If necessary, use the school's postcode as an approximate location, instead of using the child's IP address or geolocation information to determine their exact location.
- Set processing of personal information or special category data for non-essential functionality as optional and disable it by default, and allow schools to choose whether to enable it.
- Carefully consider whether it's really necessary and proportionate to collect children's biometric information, such as voice recordings, fingerprints, or facial images.

Using information only for agreed purposes

All the edtech providers we worked with used children's personal information to:

- set up individual user accounts or pupil profiles; and
- provide the core product functionality, such as logging incidents or recording learning.

Most edtech providers also used children's information for their own internal purposes, including:

- monitoring product performance;
- producing analytics information; and
- developing and testing new features or other products.

In several cases, providers also used children's information to:

- train and test AI functionality or AI-powered adaptive learning components; or
- produce anonymised information and pupil profiles for onward sharing or research studies.

Providers often couldn't demonstrate that their additional use of children's information for their own purposes was fair, as they only had access to children's information because they were a processor contracted to provide the product and service to the school. As a result, around 70% of providers couldn't show that the school or child had instructed or authorised them to use the children's information in this way.

Most additional uses of children's personal information for the provider's own purposes weren't clearly stated in written contracts with schools, written processing instructions, or other documents available to schools. As a result, schools, parents, and pupils were unlikely to be aware that children's information was being used in these ways when they used the edtech products. Therefore, they couldn't assess the privacy risks or make informed decisions about the data use.

We observed edtech providers determined the purposes and means of the additional processing, but they usually hadn't recognised that they were controllers for it. As a result, they hadn't:

- identified an article 6 lawful basis or article 9 condition for the additional processing;
- recorded it in their ROPA;
- completed a DPIA; and
- informed children and parents.

Where providers further repurpose children's information, the new purpose must be compatible with the original purpose. Otherwise, the processing doesn't comply with the purpose limitation principle in UK GDPR article 5(1)(b). A compatibility assessment is a good way to check this.

We told edtech providers to consider carefully before using children's personal information or special category data for their own purposes, and assess how additional processing is fair and lawful and document this robustly, such as in a DPIA.

If the provider determines the means and purposes in practice, the provider is the controller and must comply fully with UK data protection law. This includes:

- identifying a lawful basis;
- keeping records of processing activities;
- completing a DPIA; and
- informing children and parents transparently.

Storing information for only as long as necessary

When edtech providers were processors acting on each school's instructions as controller, some providers allowed schools to set their own retention periods for children's information. They did this by configuring the product for each school as part of set-up or onboarding. Alternatively, they provided functionality in the product for the school super-user to configure themselves.

However, in practice, we found that most edtech providers set a fixed retention period universally for all schools using their products, and schools usually couldn't change it. In around 70% of cases, providers either:

- failed to clearly specify the retention period; or
- kept children's information for an excessively long time that they couldn't justify.

This was especially common for classroom learning products.

A small number of edtech providers also retained children's information indefinitely in their products in practice, either:

- deliberately in case they might need it in the future; or
- because automatic or manual deletion cycles hadn't taken place as planned.

This meant that schools couldn't meaningfully control how long edtech providers kept children's information, so they were unable to ensure compliance with the storage limitation principle as the controller.

Further, edtech providers weren't always clear or transparent about what they would do at the end of the retention period. Some said they would delete personal information after the retention period, or they didn't state what action they would take at all. But in practice, they anonymised information and kept it for their own uses. This meant that schools, children, and parents:

- didn't know how long edtech providers would actually store the personal information; and
- couldn't always trust that the providers would delete the information when they should.

We told edtech providers to record retention periods – and the action taken at the end of the retention period – clearly and transparently in:

- written contracts with schools;
- records of processing activities;
- privacy information; and
- DPIAs.

We also asked providers to consider allowing schools to configure the product and set the retention period themselves, either through product configuration functionality or manually, as part of onboarding.

 We asked edtech providers to think carefully before choosing to anonymise information instead of deleting it. Applying anonymisation techniques to turn personal information into anonymous information counts as processing personal information. When doing so, providers must comply with UK data protection law and truly and irreversibly anonymise the information.

Outcomes

The edtech providers we engaged with agreed to:

- ensure they collect only the minimum children's personal information necessary to operate their product, and let schools decide whether to process more for additional features;
- stop repurposing children's information for other purposes that are incompatible with the original purpose for processing;
- retain information for only as long as necessary; and
- record clear actions at the end of retention periods.

Edtech providers that we followed up with have reviewed their approach to data minimisation, purpose limitation, and storage limitation. They have begun taking action to align their products with these principles. This helps to ensure that children's personal information is fundamentally better protected, and makes it significantly easier for schools to comply with the law.

Case studies

Case study: An edtech provider had a classroom learning app for use at school or at home. The app collected every child's:

- full name;
- national unique pupil number and admission number;
- date of birth;

- gender;
- ethnicity; and
- email address.

Schools could choose to share the child's:

- pupil premium or free school meals status; and
- disability status.

All other data fields were mandatory.

The provider couldn't:

- justify why this amount of personal information was necessary; or
- show that this was the minimum personal information needed for their product to work.

They also collected each child's location – specifically their city and country – using their IP address. The provider used this to authenticate users when they accessed their accounts from different locations and when the provider implemented increased security measures. However, it wasn't clear whether this was necessary.

We told them to complete an assessment to determine the personal information necessary for each element of their product. We suggested several pro-privacy alternatives that reduced the information collected and lowered the risk to children's privacy in the event of a breach.

The provider completed this review, reduced how much personal information they collected and deleted information they no longer needed. This reduced the risk to children's privacy if a personal data breach occurred.

Case study: An edtech provider used children's special category data to deliver their product and service. They repurposed some of this information for their own purposes, including:

- improving their edtech products and debugging product issues;
- testing whether new features worked in development;
- analysing product performance, user behaviour, and usage trends; and
- producing anonymous pupil profiles.

They hadn't assessed how each additional use complied with the data protection principles. Additional uses also weren't mentioned in the written contracts with schools or any written processing instructions. The provider hadn't determined that they were the controller for additional processing and therefore hadn't:

- recorded it in their ROPA;

- identified a lawful basis and article 9 condition; or
- completed a DPIA.

The provider only mentioned additional uses very broadly in privacy information, which meant children and parents were unlikely to know it was happening.

We required the provider to demonstrate how the additional processing for their own purposes complied with the data protection principles. Upon review, they determined that it wasn't fair to reuse special category data as a controller that they only had access to because of their contract as a processor. They also couldn't identify an appropriate lawful basis and article 9 condition for the additional use. As a result, they:

- stopped using special category data for these additional purposes; and
- deleted information they weren't processing as a processor.

We are continuing to work with the provider to explore alternative options that don't compromise children's privacy.

Case study: An edtech provider had decided to anonymise all children's personal information after the retention period or at the end of the contract. Their privacy information and written contracts with schools stated that they would delete or anonymise that information at the school's choice. However, in practice, the provider anonymised the information before deletion in all cases, regardless of what the school had decided.

ICO anonymisation guidance states that information is anonymous when "the data subject is not or no longer identifiable". It is pseudonymised when information that directly identifies people is replaced or de-coupled, but someone could reidentify the data by combining it with other information. Pseudonymous information is still personal information and within the scope of UK data protection law, whereas anonymous information is not. Also, applying anonymisation techniques to turn personal information into anonymous information is still processing personal information, so UK data protection law applies.

The provider supplied a detailed methodology for anonymising information. However, when we reviewed it, we found that they had pseudonymised, not anonymised, the output. They had decoupled information from unique identifiers into two separate databases, but anyone could reidentify the information by combining the databases using a reference key the provider had kept.

They hadn't recognised that they were the controller for this processing. As a result, they hadn't met any of their data protection responsibilities. They:

- hadn't identified an article 6 lawful basis or article 9 condition;
- hadn't clearly informed children or schools; and
- were retaining pseudonymous information indefinitely.

We required them to urgently review this use of children's personal information. They took immediate action to fully anonymise information they had already stored and to apply the same approach moving forward. We also followed up with them over the following six months to ensure they:

- updated their ROPA;
- updated their privacy policy and written contracts with schools; and
- completed a DPIA to assess the risks.

Case study: An edtech provider had designed their product to work without requiring any children's information at all. Schools could either let children access the service using a generic school user account or give each child an individual user account (using a pseudonym, code, or other unique identifier).

Schools could choose to share further optional personal information to enable features that required it, such as demographic information for analysis dashboards and date of birth for content tailored to age. However, this still worked with pseudonyms or codes, so sensitive information wasn't linked directly to the child's name.

Building on this approach, the provider only used children's information for the school's intended purpose of providing the educational product. They used synthetic data to develop and test new products and features and to debug performance issues. They didn't anonymise children's information, and they deleted it as agreed with each school.

These positive measures ensured that children's personal information was only processed when it was actually needed and solely for the agreed purpose of education. When schools used the edtech product without providing children's information at all, this significantly reduced the risk to children's privacy.

Further reading – ICO guidance

- Principle (b): Purpose limitation
- Principle (c): Data minimisation
- Principle (e): Storage limitation
- Anonymisation
- Biometric data guidance: Biometric recognition

Transparency

At a glance:

- We reviewed whether children, families, and schools were informed in clear and non-technical language about how edtech tools processed children's information, especially when the providers used the information for their own purposes.
- We found there was usually only general information provided about edtech products and how they used children's information. Privacy information was often missing key information about processing, or providers hadn't kept it updated.
- We told edtech providers that privacy information, public resources, and explainers must be made available to schools, families, and children, so people can make informed decisions about the privacy risks to children. Providers should produce detailed non-technical resources that explain how their products work and how they use children's information.

Findings

Providing privacy information

Transparency is key to data protection and an important part of the lawfulness, fairness, and transparency principle in UK GDPR article 5(1)(a). Organisations must be open and honest about how they use personal information, especially when the processing is complex or if it relates to a child.

When edtech providers are controllers, they must inform children about the use of their information and provide them with the information required in UK GDPR articles 13 and 14.

When edtech providers are processors and handle children's information only on the school's instructions, they should support schools to make the processing transparent. They can do this by providing relevant technical information about their products and how they process information – this may be information known only to them as the developer.

Providing this information is even more important when processing is particularly complex, or takes place invisibly in the back-end of products which schools may not be fully aware of.

Edtech providers that proactively support schools to provide the required information to children and meet transparency requirements may gain a competitive advantage by building trust with schools and the public.

We reviewed public privacy information and found that around 80% of edtech providers had published information that wasn't detailed enough to explain how their products processed personal information. There was often very limited insight into:

- how the products worked;
- what features they had; or
- how providers used children's information for their own purposes (such as developing product features or training AI functionality).

Several privacy policies used basic templates with generalised descriptions that could reasonably apply to most technology products. This made it difficult for schools to fully inform children and families. When an edtech provider is a controller, this doesn't comply with UK GDPR articles 5(1)(a) and 13.

Understanding privacy information

Most privacy information was text-based and long, which is generally suitable for adults with good literacy. But very few edtech providers produced child-friendly information or alternatives tailored to children's reading ages and understanding. Children need information in a concise and easily accessible form, using clear and plain language, to help them understand how edtech providers are using their information.

We suggested that edtech providers carry out user testing of privacy information intended for children, to get assurance that the information is clear and accessible, and children can sufficiently understand it.

Feedback from children can also help to guide product design choices, and identify the best points in the user journey to present the information.

Reviewing and updating privacy information

Edtech providers must keep privacy information up to date so that it stays accurate. Over 25% of edtech providers hadn't regularly reviewed their privacy information or resources, so they couldn't show that they had updated them when they made changes to products or processing. In every case, this meant that people received inaccurate and misleading information about the product and how it used personal information. As a result, schools were likely giving inaccurate information to children and families.

We required edtech providers to regularly review privacy information and other resources that explain their products and how they process personal information, especially when making changes to products or introducing new features.

Additional resources

Some edtech providers had proactively published additional resources on their websites or in online privacy hubs to help children, families, and schools understand how they processed children's information. Examples included:

- explanations, videos, or diagrams showing how the product and its features worked;
- simple information about what personal information providers collect and how they use it;
- non-technical descriptions of back-end processing that would otherwise be invisible to people;
- information about safeguards and safety features;
- demonstrations of privacy settings and monitoring controls for schools or families;
- FAQs addressing common questions or concerns; and
- guides to help parents and families explain information use to their children.

Around 40% of providers hadn't produced any additional resources or information about how the products worked in practice beyond their privacy policy. As a result, schools often had limited information to share with children and their families about how the products worked and how they used children's information.

Outcomes

The edtech providers we engaged with agreed to:

- provide more detailed information and resources to schools explaining how their products use children's personal information so that their products are as transparent as possible; and
- review their privacy information to make it child-friendly and keep it updated, particularly when there are changes to the features or functionality of the tool.

Edtech providers that we followed up with have updated their privacy information and now provide more detailed information about processing. This means that the use of children's information in edtech products is now more transparent, which builds trust and confidence in the use of edtech in schools.

Case studies

Case study: An edtech provider had produced a privacy policy which was available on their website and in the product.

The privacy policy was text-based and provided some detail on how the product used personal information, but it wasn't detailed enough. Several areas had missing information or only brief explanations. The policy only gave basic examples of the personal information used. It also informed readers that special category data wasn't used when it was, which was inaccurate and misleading.

Several sections of the privacy policy contained generic non-committal statements that restated basic legal principles, especially about:

- retention periods;
- international transfers;
- the safeguards in place; and
- how to make individual rights requests.

The provider didn't appear to have regularly reviewed or updated the privacy policy.

The privacy policy didn't explain how the provider used children's information in its AI features, including for training the AI. It also failed to state that the provider anonymised children's information and special category data to create child profiles for their own uses. Children, families, and schools were unlikely to know this, making it effectively invisible. They were a controller for these purposes, and therefore weren't complying with the transparency principle.

We told them to update their privacy information and provide more detailed explanations of their product. We explained what information they must include. We followed up over the next six months and reviewed the new privacy information, which was clearer and more informative. They were also developing a child-friendly privacy policy and additional resources, which they will make available on their website after user testing with children to ensure it is understandable.

Case study: An edtech provider had two privacy policies:

- A comprehensive policy intended for schools, families, and the public; and
- A simplified policy for children

Both policies clearly explained what the provider used children's information for and how they processed it. They also included detailed explanations about how the processing complied with UK data protection law and what safeguards were in place. The children's privacy policy included the same information in simple

language and used diagrams to aid understanding. Both privacy policies were easy to find because the provider signposted them:

- on their website;
- in several places within the product; and
- in every communication email to schools and families.

The provider offered additional resources on their website, including:

- product demonstrations;
- explanations of safety features; and
- information specifically for children.

If schools asked for further technical information, the provider supplied it and also added it to the additional resources available for the benefit of other schools.

This helped to ensure information about processing was easy to find and understandable, clearly informing both children and adults.

Further reading – ICO guidance

- Principle (a): Lawfulness, fairness and transparency
- The right to be informed
- Should we test, review, and update our privacy information?
- Children's code standard for transparency

Integrity, confidentiality, and security

At a glance:

- We reviewed whether edtech providers managed information security, integrity, and access risks. We also reviewed whether they had controls in place to protect children's information during collection, in transit, and at rest.
- We found that edtech providers had generally implemented information security safeguards and controlled access to children's information, but they didn't always proactively test for vulnerabilities. We also saw:
    - personal data breach processes; and
    - misunderstandings about processors needing to report all breaches to schools without delay.
- We told edtech providers to:
    - review their technical and organisational measures;
    - introduce routine vulnerability testing; and

    - carry out internal or external audits to confirm that these measures are in place and effective.
- We also required them to revise their personal data breach policies, and ensure they report all breaches of any risk level to schools without undue delay.

Findings

Technical and operational measures

Processing personal information securely and protecting it from accidental loss, destruction, or damage is required by the integrity and confidentiality principle in UK GDPR article 5(1)(f). Edtech providers must put appropriate technical and organisational measures in place to secure and protect personal information, as required by article 32. This applies to both controllers and processors.

Edtech providers typically hosted their products on third party infrastructureusing cloud servers with elastic capacity to minimise downtime or availability risks. Most had implemented a range of information security safeguards, either themselves or using a suite of safeguards and monitoring tools built into third party services.

Most edtech providers had implemented at least:

- encryption of personal information (AES 256-bit at rest and TLS 1.2 or TLS 1.3 or higher in transit);
- additional safeguards for special category data or sensitive information;
- virtual private clouds, security groups, firewalls, automatic throttling, and network access control lists to segment and protect network traffic;
- role-based access controls based on least privilege for staff, with privileged access restricted to a small number of developers;
- multi-factor authentication for staff accounts and devices, enforced for all accounts accessing children's personal information, privileged accounts, and admin actions;
- secure development and code testing;
- a robust patch management and rollback process; and
- tools to monitor threats or detect anomalies and vulnerabilities.

In discussions, leaders and operational staff showed a strong commitment to information security and a low tolerance for security risks in their products. There were only a few isolated minor gaps or opportunities to improve existing safeguards.

A significant number of the good practices we noted came from providers implementing a range of security measures. This was especially the case for

larger edtech providers (such as providers of management information systems or global edtech organisations with many products). These providers' products are more likely to be targets for ransomware or cyber attacks.

Several providers also took steps to stay updated with the latest threat intelligence. These included:

- signing up to the National Cyber Security Centre (NCSC) mailing list;
- joining industry groups and networks; or
- regularly reviewing the Open Worldwide Application Security Project (OWASP) top 10 most critical threats to web application security.

Most edtech providers conducted some automatic vulnerability monitoring. However, around 20% didn't routinely test their products for vulnerabilities or check new features and code changes before release. Most of these providers were smaller organisations providing classroom learning apps.

 We advised edtech providers to check regularly that automatic vulnerability-monitoring or incident-detection tools work properly and to make sure there are no gaps or areas where vulnerabilities go unchecked.

Security compliance checks

Alongside their own internal checks of security controls, over 60% of edtech providers carried out annual external audits of information security in their products, including penetration testing and code reviews. Many providers maintained certifications of their product and networks to recognised standards (such as ISO27001 or SOC 2), or they had joined schemes such as the NCSC's Cyber Essentials or Cyber Essentials Plus. Some providers took part in online 'bug bounty' programs and invited security researchers and ethical hackers to identify bugs and vulnerabilities in their systems. These actions all help strengthen the control environment and keep children's personal information secure.

Personal data breaches

In contrast, over 70% of edtech providers had failed to document personal data breaches or were following incorrect processes when handling them. In almost all cases, edtech providers hadn't fully understood the different responsibilities of controllers and processors when handling a personal data breach:

- Controllers must report breaches to us and notify affected people based on an assessment of the likelihood of risk.
- Processors must report all personal data breaches to the controller without undue delay after becoming aware of the breach.

We found several edtech providers that were processors whose internal policies and staff guidance restricted breach reporting. Their document said they would only report high-risk or significant breaches to affected schools or only after they had ended their own investigation first. This doesn't comply with UK GDPR article 33, which requires processors to report all breaches to the controller regardless of risk and without undue delay. In many cases, this also breached the terms of the contract between edtech providers and their schools.

A small number of edtech providers had also never logged a personal data breach or near-miss incident. While it's possible that there were no breaches or near misses, it's unlikely that this has been the case for several years. This raised concerns about whether staff were detecting or reporting breaches. Also, it wasn't clear whether leaders could manage a breach effectively, as their processes were largely untested.

We told edtech providers to record processes for managing personal data breaches in detail, including:

- definitions or examples of personal data breaches, to help staff decide whether to report or not;
- the different responsibilities for controllers and processors for handling and reporting breaches;
- how they assess the likelihood of risk and the methodology they use;
- who is responsible for notifying affected controllers, affected people, and us when required; and
- template text or communications used to notify or report personal data breaches.

We asked edtech providers to review personal data breaches and identify lessons learned. They should also consider how to avoid similar breaches in the future. High breach numbers might indicate a vulnerability or problem. Low breach numbers might suggest low staff awareness or a failure to detect breaches.

Outcomes

The edtech providers we engaged with agreed to:

- proactively test that technical and organisational measures are fully in place and effective; and

- improve personal data breach processes and ensure breaches are always reported to affected controllers, and when required reported affected people and the ICO.

Edtech providers that we followed up with have taken urgent steps to:

- put the correct processes in place for handling personal data breaches; and
- make staff aware of the legal requirements to report.

Several providers have also introduced walkthrough exercises, desktop scenarios and breach simulations with key staff and leaders. These exercises help build confidence that:

- providers will handle breaches in line with UK data protection law; and
- their staff understand what to do.

This reduces the risk of harm to children and impact on schools.

Case studies

Case study: An edtech provider had a personal data breach policy that set out the process from detection and investigation through to sharing lessons learned. They were a processor when providing the edtech product, and a controller when using children's information to analyse product performance and develop products.

The policy mixed up the different processes for handling breaches as a controller and as a processor. For example, the policy stated that the provider would report only high-risk breaches to schools (the controllers), and it didn't outline:

- how the provider would assess the level of risk; or
- who would decide whether to report.

The policy included template investigation forms to log incidents and remedial actions taken. However, it didn't record when the provider first became aware of the breach or whether they informed schools, affected people, or us. The policy also didn't include template communications for reporting breaches to controllers or notifying affected people.

We required the provider to bring their processes in line with legal requirements. We explained the different responsibilities for controllers and processors and what information they needed to record. We followed up with them in the following six months, and they had revised their policy and

templates and shared changes with all staff. This gives confidence that they will handle any personal data breaches compliantly in the future.

Case study: An edtech provider carried out an annual external independent audit and penetration test of their product. The reports identified several risks and vulnerabilities, but the provider hadn't addressed several of these for many years. In the most recent report, the external partner raised concerns that most of the previously identified issues remained unresolved.

We told the provider to review internal processes for addressing risks and vulnerabilities, and to set clear timescales and priorities based on the level of risk. They took action to quickly address outstanding issues from the external report and introduced agreed standards and timescales for resolving future issues.

Case study: An edtech provider had implemented multiple layers of vulnerability-monitoring and identification tools as part of a 'defence in depth' security approach. These tools proactively scan for anomalies and automatically notify key staff and leaders when they detect issues.

They had also:

- carried out regular internal compliance checks by leaders, annual external penetration testing, and annual external certification audits to Cyber Essentials Plus, ISO27001, and SOC 2 standards;
- reviewed and tested all code from early development using a 'shift-left' approach, and they tested beta versions with a group of schools; and
- joined a 'bug bounty' program to incentivise accredited ethical hackers to identify and report bugs and vulnerabilities.

These steps helped them identify and resolve potential security and integrity issues quickly, minimising the risks to children's personal information.

Case study: An edtech provider had designed their product with access permission functionality, so school leaders or administrators could configure and assign access permissions by role for staff.

They also required multi-factor authentication for staff user accounts with certain permissions (eg administrator rights, editing rights, or the ability to view children's information across the school). The school leader could opt out of multi-factor authentication, but they first had to agree and return a document which outlined the possible risks to children by not authenticating access to their personal information. This helped raise awareness of the benefits of multi-

factor authentication and the importance of controlling access to children's information.

Further reading – ICO guidance

- Principle (f): Integrity and confidentiality (security)
- A guide to data security
- Personal data breaches: a guide
- The role of processors in personal data breaches

Contracts and third party relationships

At a glance:

- We reviewed whether written contracts formalised data protection responsibilities and processing instructions clearly and comprehensively. We also looked at whether sub-processor use was authorised and subject to ongoing checks.
- We found that written contracts and processing instructions were often too broad, unclear, or vague. Some edtech providers hadn't obtained written authorisation or carried out appropriate due diligence before engaging sub-processors, and they hadn't regularly checked that sub-processors were maintaining agreed safeguards.
- We told edtech providers that they must:
    - have written contracts that explicitly and transparently describe the proposed processing of children's information, including comprehensive processing instructions for providers to follow;
    - get written authorisation from schools before engaging sub-processors; and
    - get assurance that their sub-processors are following contractual terms and have implemented safeguards to protect children's information to the agreed standards.

Findings

Written contracts

When a controller uses a processor to handle personal information on their behalf, they must have a written contract or other legal act in place. A processor also needs a contract if they use another organisation, such as a sub-processor, to help with processing personal information for a controller.

Written contracts are important because they set out each organisation's responsibilities as a controller or processor. Contracts must clearly include detailed information and the legally required terms about how the processor will process the personal information. They must also include specific data protection clauses set out in UK GDPR article 28. Under article 29, processors must process personal information as instructed by the controller, unless the law requires them to do otherwise.

We found that almost all edtech providers used written contracts or published terms of use with schools. The edtech provider usually provided its own template, and providers often used the same terms for all schools. However, some providers added small variations or included specific information processing details in an appendix or schedule to the contract. Most schools agreed to the contract from the time the school procured the edtech product and service. The contract rolled over until terminated by either organisation.

Although written contracts existed, around 70% of edtech providers had contracts that lacked detail or didn't include the legal requirements in article 28. Several contracts used unclear terms and data protection clauses that didn't clearly set out the responsibilities of the provider and the school. Other contracts only described the proposed use of children's personal information in broad or vague terms. Some providers told us they avoided including detailed and specific information in the contract or an attached schedule or appendix because future product changes might force them to issue new contracts. Providers often didn't review contracts, so they no longer reflected changes to the:

- products or processing;
- safeguards; and
- responsibilities of each party.

Where contracts didn't describe in detail the personal information that the provider would use, how they would process it, and the agreed minimum technical and organisational measures to secure it, we found that schools didn't give clear processing instructions or these weren't recorded. This meant that edtech providers made their own decisions on how to process children's information rather than following the school's instructions. By determining the purposes and means of processing, a processor will be considered the controller in UK GDPR article 28(10). They must therefore ensure compliance with the data protection principles and all relevant requirements in UK data protection law.

Where offering standard contracts or terms for all schools, we told edtech providers to:

- ensure that the school can meaningfully control the processing; and
- allow the school to set specific processing instructions as the controller.

Providers could achieve this by including an appendix or schedule for schools to record their specific instructions, such as:

- the data fields to process;
- the format (eg full names or initials);
- retention periods;
- default configuration settings; and
- whether each optional use or feature should be on or off; or

Providers could also build a configuration dashboard into the edtech product so the school leader or super-user has to manually set the above parameters for their school before they can import children's information into the edtech product.

Written contracts must state whether the processor deletes all personal information or returns it to the controller, at the controller's choice, as in UK GDPR article 28(3)(g). Some standard contracts and terms we reviewed didn't include this requirement or explain what edtech providers would do with personal information when the contract ended. A small number of contracts described completely different actions, removed the controller's choice, and didn't comply with the law.

Sub-processors

Processors need either prior specific or general written authorisation before engaging sub-processors, as in UK GDPR article 28(2). Most edtech providers used general written authorisation and included a contractual clause that allowed them to use sub-processors. The school accepted this when it agreed to the contract.

However, around 30% of edtech providers either hadn't obtained prior specific or general written authorisation, or had general written authorisation. But they hadn't informed schools of intended changes to sub-processors or given them an opportunity to object. This meant that schools:

- didn't always know which organisations could access their pupils' information; and
- couldn't meaningfully control the processing as controllers.

In some cases, they risked losing control of children's personal information completely.

 Edtech providers must inform schools transparently and proactively before they engage new sub-processors or change the sub-processors they already use. For example, they could contact school leaders directly by email rather than simply update a list on their website.

When they inform schools of a change, we suggest that providers describe or share the due diligence checks they have completed. This is so schools, as controllers, can feel confident that the provider continues to protect children's personal information.

Due diligence and ongoing checks

Around half of edtech providers completed due diligence checks before they used sub-processors and repeated these checks periodically, including:

- requests for processing information; and
- evidence of appropriate technical and organisational measures to secure personal information.

Providers usually followed a comprehensive checklist, and DPOs and privacy or security teams were often closely involved in reviewing the information supplied by sub-processors.

However, the other half of edtech providers didn't complete meaningful due diligence checks before they used sub-processors. They also didn't regularly check that sub-processors complied with the contract and maintained the agreed safeguards. Due diligence and ongoing checks help organisations:

- identify and mitigate data protection risks;
- address compliance issues quickly; and
- build trust and transparency.

Gaps in due diligence or ongoing compliance checks were more common among larger organisations that provided:

- management information systems;
- safeguarding systems; or
- a suite of classroom learning products.

These organisations typically used far more third parties and sub-processors, which increased the risk of issues arising. Many of the edtech providers that failed to obtain proper authorisation or inform schools of sub-processor changes also failed to complete meaningful due diligence checks before they appointed the sub-processors and gave them access to children's information.

Not all providers checked what they were agreeing to before they signed a contract with their sub-processors. A small number of edtech providers had used a sub-processor to provide AI functionality on the sub-processor's standard contractual terms. These terms stated the sub-processor would use customer information to train their AI model, which in this case, included children's information from the school the edtech provider served. The sub-processor allowed organisations to opt out, but the edtech providers hadn't done so, as they had only become aware of this during our audit.

We told edtech providers to read written contracts carefully before engaging processors as a controller or engaging sub-processors as a processor. If they are unsure what any clause means, especially anything relating to the use of children's personal information, they should check and get clarity before they agree to the contract.

Finally, 40% of edtech providers proactively provided information and evidence of their data protection compliance and safeguards directly to schools. Some shared it directly with schools or made it publicly available, such as on their website or in a dedicated online repository. Unfortunately, the majority of providers didn't do this. They only shared information reactively if schools requested it, or not at all. Providing information and evidence proactively is a positive step. It gives existing schools and prospective new schools confidence that the provider complies with contractual terms and processes children's information securely, as agreed. It also helps schools to independently complete their own due diligence and ongoing compliance checks without needing to request further information. This approach can save edtech providers time in responding to individual queries or collating information that they could have made readily available.

When edtech providers share information and evidence of compliance with schools, we suggested they include relevant documents or extracts to give further assurance. For example, they could include:

- product DPIAs;
- records of processing activities;
- relevant internal policies;
- screenshots of dashboards showing safeguard effectiveness; and
- internal or external audit reports or penetration test reports.

When providers share information on their website or upload evidence to a dedicated online repository like a 'trust centre', they make it easier for schools to stay informed. For example, providers could:

- allow school leaders to subscribe to alerts of changes; or
- tell school leaders in a newsletter or by email that new information is available.

Outcomes

The edtech providers we engaged with agreed to:

- review and improve their contracts or terms;
- improve their third-party management processes;
- be more transparent about sub-processor use;
- complete due diligence and regular compliance checks; and
- make information and evidence of their own compliance proactively available.

Edtech providers that we followed up with have made:

- contracts or terms clearer and more comprehensive; and
- more compliance information available to schools.

Many have started programmes of compliance checks with their sub-processors, starting with those with the highest risk. This is positive because schools can be more confident that providers are using and protecting children's personal information as agreed in the contract. It also reduces the risk of losing control of information in long or complex data supply chains.

Case studies

Case study: An edtech provider provided an online classroom learning product to schools. They were a processor when processing children's information to deliver the product and service. They were a controller when repurposing this information to train their adaptive learning functionality and produce anonymous pupil profiles.

They had a data sharing agreement with each school. However, these are usually for sharing information between two controllers. The agreement broadly covered data protection clauses, but it didn't give enough detail. It didn't explain the provider's proposed use of children's information and the school's processing instructions as the controller.

The agreement also contained several inconsistencies. For example, it described two contradictory actions for handling personal information if the contract ended. It also said that the provider wouldn't maintain records of processing

activities unless the school required it – however, UK GDPR article 30 requires this.

We explained what written contracts or terms needed to include so the provider could make them detailed and specific. We followed up with them in the following six months, and they had updated their contractual terms, making them more detailed and splitting them into clear sections. The new terms showed when they acted as a controller and when they were a processor. This made their use of children's personal information more transparent and clarified each party's responsibilities. They are now rolling out the updated terms to schools.

Case study: An edtech provider used several sub-processors to deliver their product and process children's personal information. Schools that used the product agreed to standard terms that gave the provider general authorisation to use sub-processors. However, the provider had recently appointed new sub-processors without informing schools.

The provider also hadn't carried out due diligence on new potential sub-processors. They hadn't asked for information or evidence to confirm that existing sub-processors were complying with contract terms and maintaining strong controls. Instead, they relied on contractual liability clauses to ensure compliance and provide redress if something went wrong.

We told them to inform schools transparently and do appropriate due diligence before engaging new sub-processors. We also told them to regularly check that sub-processors are complying with the contract and handling children's information as instructed. We followed up with them in the following six months. They had started a programme of risk-based due diligence and ongoing compliance checks with all sub-processors. This increases confidence that all parties are handling children's information correctly and protecting it as agreed. It also helps them identify and mitigate risks more quickly.

Case study: An edtech provider took proactive steps to make sure they tightly restricted and controlled third-party AI functionality in their product at all times. They had written contracts that clearly prohibited the third-party AI provider from:

- retaining children's information; or
- using school information to train, test or otherwise develop their AI.

They also checked compliance with these terms as part of their ongoing compliance checks. These measures reduce the risk that schools lose control of

children's information in complex AI supply chains. They also help prevent gaps in safeguards and protections for children.

Case study: An edtech provider proactively published compliance information in a dedicated online repository that was available from their public website. This included clear information statements and specific evidence showing how they met their contractual and data protection responsibilities. Examples included:

- internal and external audit reports, certification reports, code checks, and penetration tests;
- a complete list of sub-processors, the children's information each one could access and why, and an overview of the due diligence checks completed and when they last reviewed them;
- DPIAs for their product and product features;
- statements describing each technical and organisational measure in place to protect information, and evidence where applicable;
- widgets showing live system status and the time of the last successful back-up; and
- training videos and help articles about safety features, such as access permissions, school configuration options, or user privacy settings.

This approach helps schools to maintain control of children's information. It also builds public confidence that the provider protects and handles the children's information with care.

Further reading – ICO guidance

- Contracts
- Controllers and processors
- What does it mean if you are a processor?

Data protection management and oversight

At a glance:

- We reviewed the existing data protection management framework. This included:
  - senior leadership oversight;
  - monitoring of compliance;
  - internal policies; and
  - staff training and guidance.

- We found that some edtech providers had failed to set clear internal data protection policies. Some hadn't given staff in specialised roles the training they needed. Others didn't regularly check compliance across their organisations.
- We told edtech providers to put a robust data protection management framework in place. This should include:
    - clear and detailed policies describing key processes and responsibilities;
    - appropriate staff training and guidance for each role; and
    - regular oversight of compliance.

Findings

Technology products that process children's personal information need to be designed and developed within a robust and embedded management framework. This framework must set clear accountability for privacy and data protection. An effective data protection management framework includes:

- leadership oversight of data protection;
- appointment of a Data Protection Officer (DPO) where required;
- clear, detailed policies and staff guidance;
- appropriate data protection training for staff;
- internal checks and external audits; and
- regular reporting of compliance metrics or KPIs.

We worked with senior leaders and operational staff during our audits. We often saw that senior leaders were knowledgeable about their edtech products and were involved in making or overseeing decisions during development. This was the case in larger organisations that provided management information systems or a range of edtech products and in smaller organisations providing just one classroom learning product. Senior leaders talking openly about data protection compliance helps to promote a strong data protection culture and 'tone from the top' throughout the organisation.

Data Protection Officers

Organisations must appoint a Data Protection Officer where their processing of personal information meets the criteria in UK GDPR article 39. Most edtech providers processed children's special category data on a large scale, so they had appointed a DPO. These DPOs monitored data protection compliance and reported issues to senior leaders.

Around 20% of edtech providers didn't have an effective DPO in place when one was required. In some cases, the provider hadn't realised a DPO was required

and hadn’t appointed one. In other cases, the DPO had a clear conflict of interest or couldn’t complete their tasks in article 39 to monitor compliance properly. In these situations, we also found significant gaps in data protection compliance across several areas. These providers were required to take extensive action to improve.

We required edtech providers to review DPO appointments where there is a conflict of interest. This includes situations where the DPO:

- makes technical decisions about processing; or
- is responsible for product commercial performance or operational compliance.

A DPO in these roles can't act independently when monitoring compliance.

In smaller organisations with fewer staff members, providers could consider alternatives that protect the DPO’s independence and ability to act, such as:

- reallocating compliance and commercial responsibility to remove the conflict of interest and give the DPO the freedom to carry out their statutory tasks;
- appointing an external DPO through a service provider; or
- sharing an internal DPO across a group of organisations.

Policies and staff training

Despite senior leaders’ involvement in product development, we found that around 80% of edtech providers hadn’t formalised their approach to data protection compliance. They hadn’t set clear staff responsibilities or written detailed policies for key data protection processes. Without clear and detailed policies to guide staff, staff may not know what is expected of them or follow agreed processes consistently. This increases the risk of personal information being breached.

We also found that these edtech providers hadn’t trained staff appropriately. Many hadn’t given specialised training to key staff with data protection responsibilities. Some hadn’t even rolled out basic data protection awareness training for all staff. If staff don’t receive the right training for their role or don’t understand how to safely handle and protect children’s information, they are more likely to make mistakes or fail to report issues.

We told edtech providers to identify staff with key data protection responsibilities and record any additional or specialised training they need in a training plan or training needs analysis. This includes:

- information security training for staff who assess security risks or complete DPIAs;
- individual rights training for customer support staff;
- personal data breach management training for staff who investigate them; and
- training on handling children's information and the risks, for developers and product owners.

Internal compliance

Finally, we noted an opportunity for edtech providers to improve how they check their compliance. Internal compliance checks help confirm that staff are:

- following agreed processes;
- meeting their responsibilities; and
- keeping safeguards in place and effective.

External audits also add value because they provide an independent view of the control environment, often against recognised national or international standards.

Almost 40% of edtech providers didn't complete regular internal compliance checks or schedule periodic external audits, and some did neither. This was a common finding among the largest organisations we worked with, such as providers of management information system or those offering a range of edtech products.

This was also a common finding for several recent startups providing an edtech product.

We suggested that edtech providers set data protection compliance metrics or KPIs to identify trends and monitor emerging risks. For example, we suggested monitoring:

- numbers of personal data breaches and near-miss incidents and how long it took to report, investigate, and remedy them;
- numbers of individual rights requests received and how long it took to respond to them; and
- numbers of complaints or requests for further information from schools, or families or children.

We suggested edtech providers use the ICO's data protection audit toolkits to internally audit their compliance with UK data protection law and our guidance. A wide range of toolkits and resources are available for organisations to use.

Outcomes

The edtech providers we engaged with agreed to:

- review and improve their data protection management framework where needed;
- ensure staff receive appropriate data protection awareness training, and specific or specialised training relevant to their responsibilities; and
- monitor compliance regularly through internal checks, external audits, and relevant KPIs or metrics.

The providers we followed up with have taken steps to promote data protection awareness and build a positive organisation culture. This is positive because staff and leaders are more aware of:

- the importance of handling children's information carefully; and
- the risks and consequences of not doing so.

Case studies

Case study: A large edtech provider offered a range of products and employed 150-200 staff across several teams. They had appointed a DPO, but the DPO hadn't received training on their statutory tasks and didn't have enough time and resources to monitor compliance effectively.

The provider also didn't have data protection or product development policies. Staff received only one basic data protection module as part of mandatory annual training for all staff, regardless of their role. They relied on existing staff knowledge of processes and past decisions, rather than having a clear policy framework or structured training plan.

We told the provider to improve their data protection management framework, starting with appointing a DPO with the right position, training, and capacity, who could oversee data protection effectively. We followed up with them in the following 12 months. They had appointed a new internal DPO who had received specific training on their statutory tasks and was carrying them out. They had also:

- produced and shared a data protection policy with all staff; and
- completed a training needs analysis and were rolling out relevant training by team and job role.

These changes led to significant improvements in how they developed their products and managed potential risks to children.

Case study: A small edtech provider offered one product and had a very small team. They had designated a senior leader as DPO. However, this leader had also developed the product and was accountable for commercial performance. This was a significant conflict of interest with their statutory DPO tasks. Although the DPO monitored data protection compliance regularly, they were essentially checking their own work, which meant the checks weren't independent.

We told the provider to review their DPO appointment and ensure they could effectively fulfil their statutory tasks. We followed up with them in the following six months. They had:

- employed a different staff member as DPO to remove the conflict of interest; and
- used an external service provider for independent expert oversight and additional capacity at low cost.

They told us this change had been instrumental in improving their data protection compliance in several other areas.

Case study: An edtech provider was a larger organisation with a range of edtech products and 150-200 staff across several teams.

The provider reviewed data protection and privacy at senior leadership and team meetings. Product changes and uses of children's personal information required the approval of the leader with responsibility for data protection. The privacy team held open office hours where staff could discuss ideas, raise queries or get advice. Staff had access to a library of bite-sized data protection policies that set out general principles to follow as well as specific step-by-step guidance. Leaders completed ongoing internal compliance checks on a cycle, and they undertook independent external audits and certification of their product annually, using experts specialising in privacy in educational settings.

These measures helped to embed a positive culture where protecting children and their information was at the heart of decisions.

Case study: An edtech provider was a smaller organisation with only one product and a very small staff. They had taken steps to embed data protection as a guiding principle for all staff.

Every senior leader was jointly and individually responsible for data protection. Data protection compliance was a standing agenda item and discussed at regular all-staff briefings. All staff had completed detailed mandatory UK GDPR and cybersecurity training, refreshed annually.

Staff members also received additional relevant data protection training specific to their responsibilities or team. If a staff member hadn't completed training, the provider suspended system access (or didn't grant access to the system at all). This ensured that untrained staff members didn't have access to children's personal information. The provider also undertook several independent external audits and certifications, which were staggered across each quarter to promote continuous year-round compliance.

Further reading – ICO guidance

- Data protection officers
- Accountability principle
- Data protection audit toolkits

Data protection impact assessments and risk management

At a glance:

- We reviewed whether edtech providers had:
  - completed a comprehensive Data Protection Impact Assessment (DPIA) for their product when required; and
  - effectively mitigated risks to children before processing their information.
- We found that DPIAs often lacked detail, were missing required information, or hadn't properly assessed and mitigated risks to children. In some cases, providers hadn't completed a DPIA at all.
- We told edtech providers to ensure that DPIAs are meaningful and describe the processing, safeguards, and risks to children in detail. Providers must mitigate and manage risks robustly. We expect DPIAs to be done early in product development and before processing, and reviewed regularly or when processing changes.

Findings

A DPIA is required when processing is likely to result in a high risk to people's rights and freedoms. In particular, UK GDPR article 35(3)(b) requires a DPIA before processing special category data on a large scale.

We have also published a list of processing operations that require a DPIA under UK GDPR article 35(4). Of these, 'innovative technology' and 'targeting of children' (including offering online services to children) are likely to apply to the use of children's information in edtech products.

Edtech providers must do a DPIA when:

- they process children's information in their products as a controller; and
- the processing involves innovative technology or offering online services to children.

They must also complete a DPIA before processing children's ethnicity and health information on a large scale as a controller, such as for analysing product performance or training AI features. Providers should still consider completing a DPIA for the proposed use of children's personal information, in order to assess and mitigate risks to children.

Doing a DPIA

We found that over 40% of edtech providers hadn't done a DPIA at all for their product. Generally, this was because providers had incorrectly decided that they were a processor and didn't need to complete a DPIA. This was the case even though they were repurposing children's information for their own purposes and were therefore a controller.

Positively, 20% of edtech providers had completed a DPIA that met the legal requirements. Strong DPIAs:

- list all the personal information the provider will use;
- explain in detail exactly how providers will use the information;
- describe comprehensively the technical and organisational measures in place to protect children's personal information; and
- assess the potential risks to children and set out clear mitigating measures to reduce the likelihood and severity of those risks.

We asked edtech providers to consider completing a DPIA, even when one isn't legally required. Doing so helps them:

- identify and mitigate the increased risks that come with handling children's information; and
- check that their technical and organisational measures are in place and effective.

We told edtech providers to document the requirement to do a DPIA in their relevant policies and product development roadmaps and to remind staff to start DPIAs early in product development.

Assessing the risks

Around 80% of edtech providers hadn't completed a sufficiently detailed DPIA for their use of personal information. This meant that they weren't complying with UK GDPR article 35, and in many cases, their processing also failed to meet the requirements of other parts of UK data protection law.

Nearly half of the DPIAs we reviewed were missing required information in the provider's template document or had gaps where the provider had skipped questions. Many contained only basic information about the product. Some didn't describe the use of personal information, the proposed safeguards or the product and its functionality in enough detail to be useful. Few DPIAs included any commentary, justification, or analysis of development decisions made or the approach taken to compliance.

DPIAs must assess risks to the rights and freedoms of the people whose information will be processed. Over half of edtech providers hadn't fully assessed the risks to children, or they had only assessed risks relating to security or corporate risks to their organisation. Others had identified risks but hadn't implemented mitigating measures or managed risks effectively. In many cases, providers had not checked regularly to see whether:

- their mitigating measures were in place; or
- they were effectively reducing the risk to children.

Reviewing and approving the DPIA

Providers must review their DPIAs regularly, especially before implementing product or feature changes, to ensure they stay updated and accurate. Over half of edtech providers hadn't reviewed their DPIA regularly. As a result, many DPIAs contained significantly out-of-date and inaccurate information about the use of personal information or safeguards. Where schools relied on information from edtech providers to do their own DPIA, this had a significant impact on the school's own compliance as a controller.

We suggested that edtech providers make DPIAs or detailed information about products, how they work, and the safeguards in place publicly available. This is so schools can benefit from their technical knowledge as the developer of the product when completing their own DPIA. Providers should not charge a fee for providing additional information that schools need, as this might discourage them from doing due diligence or prevent them from adequately assessing the risks.

We told edtech providers to check regularly that the agreed mitigating measures are fully in place and working effectively. This could take place alongside regular reviews of the DPIA.

Around 70% of edtech providers didn't have proper oversight and approval for their DPIAs. Common issues included:

- missing advice from DPOs or privacy leads;
- limited consultation with key internal stakeholders; and
- no agreed process for completing DPIAs.

In other cases, senior leaders hadn't reviewed or approved DPIAs, or they had signed them off despite missing information. As a result, staff members responsible for protecting children's information weren't always aware of the agreed safeguards or risk mitigations that needed to be in place. This significantly increased the risk of a personal data breach involving children's information.

Outcomes

The edtech providers we engaged with agreed to:

- complete a DPIA for their edtech product or improve their existing DPIA;
- assess the risks to children of using their information and manage those risks robustly; and
- review their DPIAs regularly, especially before making changes to the product or to how they use children's personal information.

Edtech providers that we followed up with have now provided a more detailed and robust DPIA for their edtech product. This means that potential risks to children's rights and freedoms have now been better assessed and mitigated.

Case studies

Case study: An edtech provider hadn't completed a DPIA for processing in their edtech product. This is because they believed this processing was not likely to result in high risks to children.

They were a processor when providing the core educational product and service to schools, but they were a controller when reusing children's information to:

- develop the product; and
- train the AI-powered adaptive learning technology.

This processing included special category data such as children's ethnicity and health information from a large number of schools, which requires a DPIA under UK GDPR article 35(3)(b). The product also included significant AI functionality, which is an example of innovative technology on our list of processing operations that require a DPIA under article 35(4).

We told them to assess their use of children's personal information in a DPIA. We followed up with them in the following 12 months and reviewed their completed DPIA. As a result of completing a DPIA, they:

- introduced several new safeguards;
- implemented changes to their AI technology; and
- produced additional information resources explaining the AI technology to schools and families.

Their customer support staff were also better able to inform schools about the product.

Case study: An edtech provider had completed DPIAs for each of their products. However, they hadn't reviewed them since before 2020. As a result, much of the technical information about the products and the use of children's personal information was significantly out of date and inaccurate. Therefore, the provider hadn't assessed and mitigated the new risks or changes to existing risks.

We told them to review their DPIAs and establish a process to regularly review DPIAs alongside product changes in the future. They took action to review and update DPIAs. They also introduced quarterly reviews of DPIAs and risks within product teams.

Case study: An edtech provider had completed DPIAs for each product feature and component. The DPIAs were very detailed. They explained how the processing would comply with each data protection principle and adhere to each standard in the Age appropriate design code. The provider had also consulted relevant internal teams, stakeholders, department heads, and external independent children's privacy experts, and recorded their feedback in each DPIA.

This resulted in a robust assessment of the potential risks to children, including:

- excessive product use or intrusive monitoring of children;
- unapproved processing;
- inappropriate content being available to children; and
- accidental use of nudge techniques.

The provider mitigated these risks by introducing:

- moderation tools;
- parental controls and oversight accounts; and
- restrictions on messaging functionality.

Senior leaders had to approve each mitigating measure before they considered the risk sufficiently reduced to proceed.

Case study: An edtech provider had produced a DPIA for their product. The DPIA had been reviewed during quarterly meetings between the DPO and product team, and it was also reviewed before launching product changes. The provider used a privacy compliance system that:

- tracked and recorded changes;
- prompted regular reviews; and
- provided updated DPIAs to product team members and other relevant stakeholders.

This helped to ensure all staff handling children's information were aware of how to use the information and what safeguards needed to be in place.

Further reading – ICO guidance

- Data Protection Impact Assessments
- DPIA template

Data protection in product development

At a glance:

- We reviewed product development processes and checked that edtech providers had designed their products to safeguard children's information and support children's information rights.
- We found that not all edtech providers could show how they had prioritised data protection in product development. We saw examples of providers rolling out new features or AI functionality that were set to be 'on' by default. We also observed products with hidden areas where children's information rights couldn't be fully actioned.
- We told providers to design and develop their products using a robust internal framework that puts the protection of children's information, privacy and rights at the heart of every decision. We also told them to:
    - launch new features or processing turned 'off' by default;

- introduce ways for schools to configure products to their own requirements; and
- ensure that individual rights requests can be actioned fully in all parts of their product.

Findings

Product design and development

Edtech providers must design and develop their products with the child, their rights and their privacy at the heart of every decision made. UK GDPR recital 38 says that:

> "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data".

When edtech providers are controllers, they must put in place appropriate technical and organisational measures to protect information and safeguard children's rights. This is data protection by design and default and is required by UK GDPR article 25. Edtech providers must also be able to demonstrate their compliance, which is the accountability principle in article 5(2).

When edtech providers are processors and following the school's instructions, they should still consider children's rights to privacy when designing and developing their products. Edtech products that protect children's information by design and default are more likely to be viable for schools to use. This avoids data protection compliance becoming a barrier to schools procuring and using the product.

 We told edtech providers to add prompts, milestones, or key activities into product development processes and roadmaps. This will help ensure they consider data protection and risks at each stage of product development.

All edtech providers we engaged with told us that children's privacy and protecting children's information were important considerations when developing their products. However, nearly 80% of providers couldn't fullyshow us how they had integrated data protection fully into products or meaningfully considered children when making design decisions.

Many providers offered edtech products with a standard 'one size fits all' configuration or with all functionality or processing as a bundle, which schools had to accept in order to use the product.

Without clear records or guardrails to guide product developers, there is a risk that the protection of children's information:

- isn't a primary consideration in development; or
- is deprioritised in favour of releasing new product features or commercial interests.

For example, several edtech providers had recently launched AI-powered features such as virtual assistants or adaptive content in their products. However, in many cases we found gaps in safeguards for these AI features, especially where they relied on third party AI.

Positively, some providers had kept comprehensive records of product design decisions, such as by using:

- internal collaboration software or ticket systems to document and track changes; or
- 'red lines' with detailed rationale.

Others had:

- designed their products to be highly configurable by schools; or
- turned off all non-essential functionality or use of personal information by default until a school chose to activate it.

These approaches help schools meaningfully control how providers use children's personal information. Providers of safeguarding products in particular could clearly demonstrate the steps they had taken and why.

We suggested ways for edtech providers to record decisions made during product development clearly and comprehensively, such as in:

- internal webpages;
- tickets; or
- a DPIA.

Providers could also document:

- their analysis and justification of the options considered; and
- how they have meaningfully taken into account input from subject matter experts and stakeholders.

We asked edtech providers to consider design options or configuration settings that would help each school to tailor the product and use of children's personal information based on their needs, such as:

- the format or amount of information collected (eg full names or only initials);
- visibility of child names;
- retention periods;
- toggleable optional data fields; and
- toggleable optional functionality.

Age appropriate design code

Our Children's code and education technologies guidance explains that edtech providers that provide online services to children through a school, and that process children's information beyond the instructions of schools as a controller, are in scope of the children's code (or Age appropriate design code). Although we didn't review whether edtech providers had followed the children's code in this work, some had determined their product was within the scope of the code and had taken steps to follow the code's standards. These products usually allowed schools to set their own retention periods and turn off unwanted functionality or use of children's personal information. They also included high privacy default settings and monitoring controls for staff or families.

Individual rights

We found that edtech providers hadn't always considered people's rights when designing their products. Around 30% of providers hadn't given schools the functionality they needed to fully action individual rights requests independently. Or there were hidden areas within products where children's personal information couldn't be retrieved or erased.

Schools often had to ask providers for extra support with access and erasure requests. This takes considerable time and increases the risk of missing the statutory response time of one calendar month. When schools were unaware of processing taking place in hidden areas – such as behind the scenes or in the back-end – they also risked failing to meet their transparency obligations. This was a common issue for almost half of the providers of management information systems that hold large volumes of personal and sensitive information about children for many schools.

We told edtech providers to implement self-service tools that schools can use when handling individual rights requests, such as tools that let schools:

- export a full copy of the child's information in a usable format, including all back-end or behind-the-scenes use;
- change or delete personal information held about the child; or
- pull through updates where they import information from their management information system.

Outcomes

The edtech providers we engaged with agreed to:

- improve their internal framework for the design and development of edtech products and put the protection of children's information and privacy at the heart of decision-making;
- record product development decisions and the rationale for the chosen approach; and
- introduce functionality for schools to meaningfully control how they process children's information and respond fully to individual rights requests.

Edtech providers that we followed up with have taken steps to include data protection in their product development processes. This means that they will design and develop new features or changes to products with the protection of children's information as a key priority.

Case studies

Case study: An edtech provider had a product development process and policy, with clear milestones for reviewing design decisions. However, neither the policy nor the template documents (eg checklists) mentioned data protection requirements. There were no prompts for the developers and product team staff to:

- complete a DPIA;
- take steps to protect children's privacy and information;
- record decisions about product features or safeguards; or
- consult the DPO.

As a result, they couldn't show how they had built the protection of children's information into their product from the earliest stages of development and throughout its lifecycle.

We told them to:

- integrate data protection into their product development policy;
- add milestones for completing a DPIA and consulting the DPO; and
- record design decisions that affect data protection and children's privacy.

We followed up with them within 12 months. We saw evidence that the DPO was now fully involved in product changes and signed off on changes before

launch. They had also completed DPIAs for their product, which had prompted a full review of the safeguards in place.

Case study: An edtech provider had added several AI-powered tools to their product. These tools generated and personalised learning content for each child. The provider had focused on improving user experience when developing these features, but it was unclear how they had monitored or addressed fairness and potential bias. They hadn't completed DPIAs for the product or AI features. They also had gaps in safeguards when using the third-party AI.

We told them to:

- complete a DPIA;
- monitor for fairness and bias in personalisation of content; and
- make their use of personal information by AI transparent in their privacy information.

We also suggested several safeguards for AI use. The provider completed a DPIA and introduced an AI policy to guide their use of AI in their products. They also started a full review of the safeguards to protect children's information when using AI features.

Case study: An edtech provider had taken several practical steps to protect children by default when they used the edtech product. The provider turned off all non-essential features by default. Privacy settings were available and set to high privacy by default. Each child's information and user profile were only available to the child and relevant school staff.

They had also set up a community of ambassador schools. These schools tested upcoming features and product changes and gave feedback before the provider rolled them out to all users. This helped to ensure the schools had meaningful control over their own processing as controllers. It also ensured the provider developed the product with schools' data protection compliance in mind.

Case study: An edtech provider had a rigorous product development process. Proposed changes had to pass through several stages of review before approval. From the outset, the provider embedded data protection, privacy, and security considerations and safeguards. Privacy staff had regular touchpoints with product teams throughout the development lifecycle and launch.

This process meant that schools had a product with built-in tools to access, rectify and erase children's information themselves in response to individual rights requests. Schools could also request extra help by raising a ticket with their customer support team. This meant schools could effectively manage their

data protection responsibilities and avoid unnecessary delays when responding to people.

Further reading – ICO guidance

- Data protection by design and default
- Considering data protection in practice
- A guide to individual rights
- Age appropriate design: a code of practice for online services
- The Children's code design guidance
- Artificial intelligence
- Automated decision-making and profiling

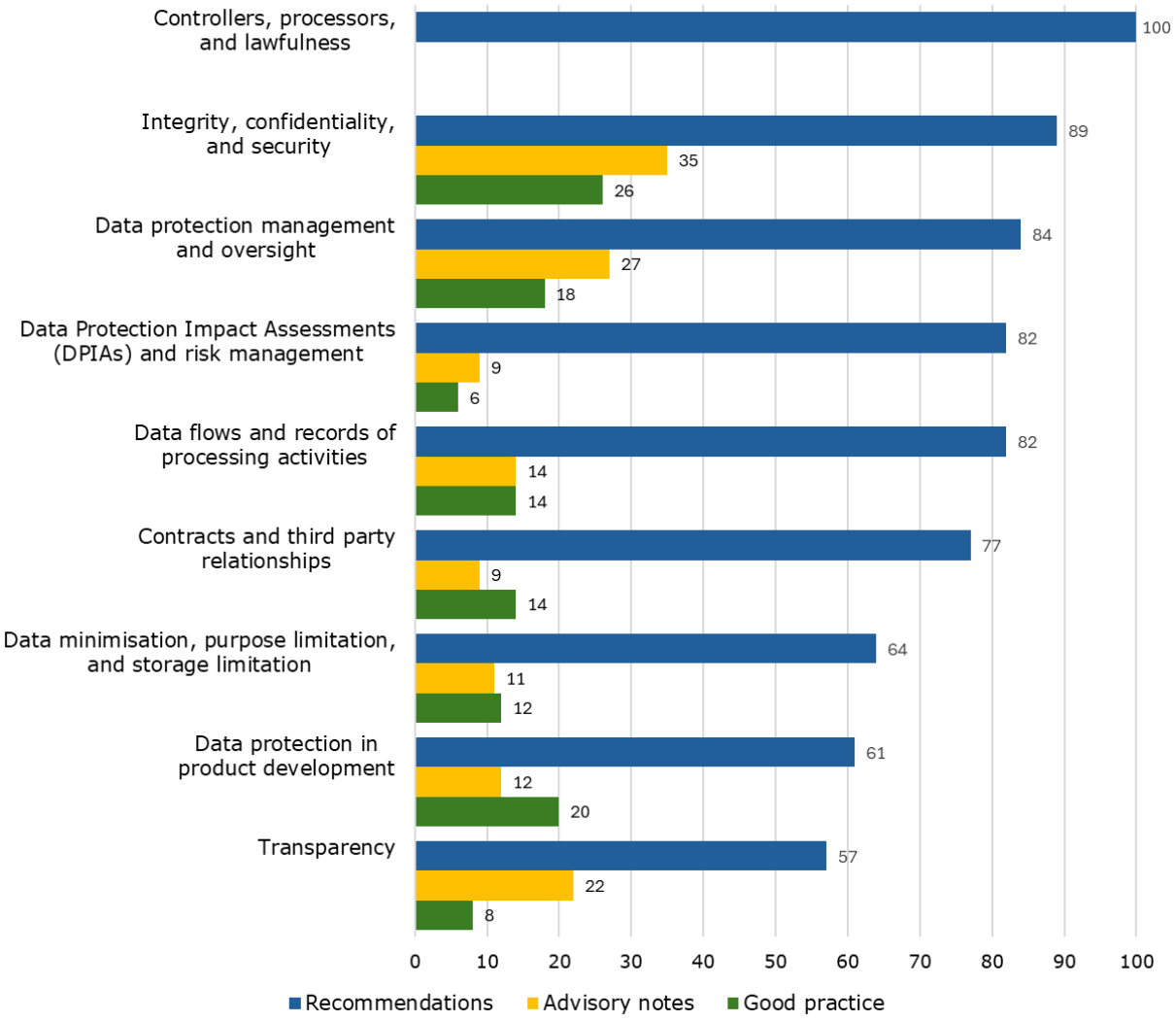
Impact and next steps

How did our audits have a positive impact?

Each edtech provider received an individual audit report that identified specific opportunities and recommendations to improve data protection compliance and enhance their processes. In total, we made:

- **596 recommendations** to improve data protection compliance or processes;
- **139 advisory notes** offering general observations and advice; and
- **118 good practice notes** where edtech providers had taken clear positive measures to protect children's information.

These were broken down by area as follows:



We recorded controllers, processors and lawfulness separately in the graph because findings in these areas often stemmed from findings in other areas.

We asked all edtech providers we engaged with to respond to our recommendations and tell us what action they would take. All providers responded positively and were willing to take action to better protect children's information on a voluntary basis. **Providers accepted 98% of our recommendations and set clear actions to address them.** This is a positive step in building the trust of children, families and schools.

After each audit, we asked edtech providers for feedback on their experience and the value added:

- **76%** said that engaging with us helped them reduce data protection and privacy risks in their products.
- **75%** said we helped them further understand the requirements in UK data protection law.
- **83%** said the audit raised awareness of the importance of protecting children's information across their organisation.

Providers also offered the following comments about working with us:

- "The audit process was efficient and the audit itself was thorough and was conducted professionally."
- "It was collaborative and a great experience overall."
- "We found the audit a great way to reflect and revisit all our policies, processes and to ensure that we are following best practice at all times. The ICO team were all a pleasure to work with, very clear with their requirements and accessible in terms of any further questions we had."
- "The overall process and experience was very positive, the ICO team were very approachable and easy to work with."
- "It helped focus our minds on what external stakeholders and regulators see to be the most important aspects in this area."
- "As a small business, with small numbers of employees, the audit has made us realise the importance of documenting and recording all decisions made when it comes to data protection by default, so that we can evidence this if ever needed in the future, and to help improve internal awareness/communications, particularly as the business and teams grow."
- "The audit highlighted that we may not always provide easy to understand data processing explanations to customers."
- "The audit was very helpful to us in finalising our understanding of controller/processor relationships, particularly the grey areas where we could be seen as a data controller or a data processor for certain customers depending on how they use our platforms."
- "We are able to implement all recommendations, and none are particularly challenging to implement from a technical or administrative

perspective. However, all take time and new/improved/modified process to implement, which can be challenging from a resource to task perspective."

- "Some items have required changes to processes – these take time and are difficult to implement as humans get comfortable with what has been."
- "We have made many internal improvements, especially in the way we document GDPR/data protection compliance."

What happens next?

We followed up with 12 of the 28 edtech providers where the data protection risks were highest. We asked them to give us further information and supporting evidence to show how they are addressing our recommendations and completing the agreed actions.

We saw a positive response to our intervention. Edtech providers took action to improve data protection compliance in their products. We worked with these providers for up to 12 months to support them and guide their products into compliance. We are reviewing progress and supporting evidence in key risk areas to confirm that they have completed the agreed actions. We will only step away once we have seen clear evidence that risks to children have reduced.

We will continue to regularly monitor the edtech sector. We will hold edtech providers to account if they fail to comply with UK data protection law and cause continued risk to children.

The findings from this audit programme support a broader understanding of data protection risks and practices in the edtech sector. We're continuing to work with the UK government on secondary legislation that will require us to produce a new code on the processing of children's personal information in digital systems in education settings. These findings will help inform the development of that code.