

POLICY ANALYSIS

THE NEW SAFEGUARDING INFORMATION-SHARING DUTY

*Understanding the new statutory
duty, child protection and parental
rights*

England | September 2026



protectandteach.org



Part 1:
**Safeguarding, parental rights and the expanding
state role**

Key findings

- The new duty creates a positive obligation to share relevant information; it is not merely permission to share.
- It operates below the traditional significant-harm threshold and extends into early help, prevention and unmet welfare needs.
- Parents do not have a veto over lawful information-sharing, but voluntary Family Help remains voluntary.
- **The statutory wording relies significantly on professional judgment;** particularly “relevant”, “promoting welfare”, “may facilitate” and “more detrimental”.
- The principal **implementation risks are inaccurate or unverified information becoming embedded across systems, professional opinion being mistaken for fact, context being lost during summarisation**, different agency systems retaining different versions, and families becoming less willing to seek early help.
- Data-protection, proportionality, accuracy, security and rectification duties remain. Better sharing therefore needs to mean better-quality sharing, not simply more sharing.

Protect & Teach’s central conclusion:

The new duty addresses a genuine safeguarding weakness, but its success will depend heavily upon how rigorously organisations preserve relevance, provenance, accuracy, proportionality and context.

Part 1 of Protect & Teach's series on safeguarding, parental rights and the expanding state role

From **30 September 2026**, a new statutory information-sharing duty applies in England under section 16LA of the Children Act 2004, inserted by section 4 of the Children's Wellbeing and Schools Act 2026.¹ The commencement regulations bring both the new information-sharing duty and associated information standards into force on that date.²

The stated objective is understandable and important. Children can be harmed when information that might have changed a safeguarding decision remains fragmented across schools, health services, police, local authorities and other agencies. The Department for Education says the new statutory guidance is intended to promote more consistent implementation and support a **"cultural shift"** in how information-sharing is understood and practised across safeguarding sectors.³

Protect & Teach starts from a straightforward principle: **necessary information-sharing is an essential part of safeguarding children.**

Professionals should not be paralysed by uncertainty about data protection or consent when relevant information genuinely needs to be shared to protect a child.

But good safeguarding is not simply synonymous with **more information being shared.**

The new statutory duty extends beyond circumstances in which abuse or significant harm has already been established. It applies where a professional considers information relevant to **"safeguarding or promoting the welfare"** of a child and considers that disclosure may facilitate another relevant organisation's safeguarding or welfare functions.⁴

¹ Children's Wellbeing and Schools Act 2026, s 4, inserting Children Act 2004, ss 16LA–16LB.

[Legislation.gov.uk](https://legislation.gov.uk)

² Children's Wellbeing and Schools Act 2026 (Commencement No. 2) (England) Regulations 2026, reg 6: sections 16LA and 16LB come into force on 30 September 2026. [Legislation.gov.uk](https://legislation.gov.uk)

³ Department for Education, *Information sharing duty statutory guidance: consultation outcome*, 10 September 2026. DfE describes the guidance as intended to promote consistent implementation and support a cultural shift across sectors. [GOV.UK](https://gov.uk)

⁴ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4. [Legislation.gov.uk](https://legislation.gov.uk)

That can encompass early help, prevention, emerging needs and circumstances that have not reached the statutory threshold for child-protection intervention.

The central policy question is therefore not whether professionals should ever share information without parental consent. They already could, and sometimes plainly must.

It is:

Has the new duty improved the ability of professionals to protect children while preserving appropriate safeguards around relevance, proportionality, accuracy, privacy and family autonomy?

That question matters because both **under-sharing and over-sharing can harm children.**

Failure to connect information can leave abuse or exploitation unidentified. But inaccurate, irrelevant or poorly contextualised information can also spread across several organisations, affect later decisions, damage trust between families and professionals, and prove difficult to correct.

The effectiveness of the new regime therefore depends not only on whether practitioners share information, but on **what they share, why they share it, how they record it and what happens to it afterwards.**

1. What has actually changed?

New section 16LA creates a positive statutory **duty to share information** in defined circumstances.

The section applies where a relevant person:

1. holds information about a child, or information about another individual which relates to that child; and
2. considers the information relevant to **safeguarding or promoting the welfare of the child**.⁴

Where those conditions are satisfied, the person must ensure the information is disclosed to another relevant person **“if and only so far as”** they consider the disclosure may facilitate the recipient's relevant safeguarding or welfare functions.⁵

There is an important exception. The duty does not apply where the practitioner considers that disclosure would be **more detrimental to the child than not disclosing the information**.⁶

The legislation also provides that a disclosure made under the section does not breach an obligation of confidence owed by the person making it.⁷

That last provision is significant. It removes professional confidentiality as a barrier to disclosure where the statutory duty itself is properly engaged.

It does **not**, however, remove the continuing requirements of data-protection law, nor does it permit unrestricted access to records.

The change is therefore better described as: **a move from lawful discretion to a positive duty in specified safeguarding and welfare circumstances**

rather than as a new general permission to share children's information.

Before 30 September 2026, safeguarding information could already lawfully be shared without consent in appropriate circumstances. Existing safeguarding and

⁵ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4. [Legislation.gov.uk](https://legislation.gov.uk)

⁶ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4.

⁷ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4.

data-protection guidance repeatedly makes clear that data protection should not prevent necessary safeguarding disclosures.⁸

What Parliament has now done is require sharing where the **new statutory test is satisfied**.

2. Who does the duty cover?

The duty extends across a substantial part of the safeguarding system.

The legislation captures bodies already subject to safeguarding duties under section 11 of the Children Act 2004, designated education and childcare agencies, and certain organisations delivering relevant services on their behalf.⁹

The DfE's statutory guidance identifies relevant sectors including:

- local authorities;
- integrated care boards;
- NHS trusts;
- police;
- education;
- early-years providers;
- prison and probation services;
- youth justice services;
- youth custody services;
- GPs, dentists and other primary-care providers.¹⁰

This breadth is deliberate.

The policy is intended to reduce situations in which different organisations each hold one part of a child's story but no professional can see the whole picture.

That is an obvious safeguarding advantage.

But it also means information can potentially move through a **large and technically diverse network of organisations**, each with its own recording systems, professional cultures, retention arrangements and access controls.

⁸ Information Commissioner's Office, *A 10 step guide to sharing information to safeguard children*. The ICO states that data-protection law permits appropriate information-sharing to identify and safeguard children at risk of harm. [ICO](#)

⁹ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4.

¹⁰ Department for Education, *Information sharing to safeguard children and young people*, statutory guidance, updated 10 September 2026. [GOV.UK](#)

That becomes important later when considering accuracy, corrections and data security.

3. Why Government says the new duty is needed

The policy rests on a longstanding safeguarding problem.

- A child may come into contact with several agencies, none of which holds enough information independently to identify the full level of risk.
- A school might know that attendance has deteriorated.
- A GP may know about repeated injuries.
- Police may have attended domestic incidents.
- Another service may know about substance misuse, exploitation or previous concerns.

Viewed separately, each item may appear insufficient to justify serious intervention.

Viewed together, they may reveal a pattern.

This is one reason safeguarding guidance has long encouraged appropriate information-sharing, and the 2026 reforms seek to move professional practice towards **earlier identification and intervention rather than waiting for crisis.**^{11 12}

That policy objective should not be dismissed.

A safeguarding regime in which practitioners wait until abuse has been conclusively established before communicating would itself create danger.

The difficult question is how early sharing should begin, and how much uncertainty the system should tolerate.

¹¹ Department for Education, *Information sharing duty statutory guidance: consultation outcome*, 10 September 2026. DfE describes the guidance as intended to promote consistent implementation and support a cultural shift across sectors. [GOV.UK](#)

¹² Department for Education, *Working together to safeguard children 2026*, and 2026 summary of changes, including the move towards integrated Family Help and strengthened multi-agency arrangements. [GOV.UK](#)

4. The new duty is wider than “child protection”

This distinction is fundamental.

Under section 47 of the Children Act 1989, a local authority's child-protection enquiry is associated with **reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm.**

Section 16LA uses a much broader concept.

It concerns information relevant to:

“safeguarding or promoting the welfare of the child.”¹³

The statutory guidance and consultation materials make clear that the new regime is intended to operate in circumstances involving **early help, prevention and emerging need**, not merely once statutory child-protection thresholds have been reached.^{14 15}

This creates something of a continuum:

known or suspected serious harm:

- **credible emerging safeguarding risk**
- **early welfare concern**
- **unmet need or preventive support**

The new duty can potentially operate across that continuum.

That may allow genuinely valuable early intervention.

But it also means the strength of the underlying evidence may differ enormously from case to case.

The safeguards therefore need to work just as effectively at the low end of the continuum as they do in obvious child-protection cases.

¹³ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4. [Legislation.gov.uk](https://www.legislation.gov.uk)

¹⁴ Department for Education, *Information sharing duty statutory guidance: consultation outcome*, 10 September 2026. DfE describes the guidance as intended to promote consistent implementation and support a cultural shift across sectors. [GOV.UK](https://www.gov.uk)

¹⁵ Department for Education, *Information sharing to safeguard children and young people*, statutory guidance, updated 10 September 2026. [GOV.UK](https://www.gov.uk)

How this could work in practice

Example A – a clear safeguarding disclosure

A child tells a teacher: **“Mum’s boyfriend hit me last night.”**

The teacher does not have to investigate the allegation to a criminal standard before acting.

The information may plainly be relevant to safeguarding the child, and sharing it with the school's DSL and, where appropriate, children's social care or police may be necessary.

A parent cannot prevent an otherwise lawful safeguarding disclosure simply by saying: **“I do not consent to you telling social services.”**

This is where the policy justification for decisive information-sharing is strongest.

Waiting for parental consent could expose the child to further harm.

Example B – pieces that only become significant when combined

Police become aware that a 14-year-old has repeatedly been seen with older teenagers associated with county-lines activity.

The school separately knows the child has begun disappearing during the school day and has become increasingly absent.

Neither piece of information independently proves exploitation.

But together they may materially change the assessment of risk.

This illustrates the strongest rationale behind the new duty: **the system should be able to join up weak but relevant signals before serious harm becomes obvious.**

That is preventive safeguarding rather than retrospective safeguarding.

Example C – welfare rather than abuse

A child with additional needs has become increasingly anxious and is attending school less frequently.

During a conversation with school staff, the parent, or parents explain that they are struggling personally and finding it increasingly difficult to manage appointments and routines.

There is no allegation of abuse.

There may nevertheless be an unmet need for support.

Under the new framework, relevant information could potentially be shared with another service if the practitioner considers that doing so may facilitate that service's safeguarding or welfare function.¹⁶

That could result in genuinely helpful early intervention.

But this example is materially different from Example A.

There is no allegation of violence, exploitation or neglect.

The justification for disclosure rests much more heavily on professional judgment about **welfare and unmet need**.

That is precisely why the breadth of the new duty deserves scrutiny.

5. The importance of the words “considers” and “may”

The statutory wording places considerable responsibility on professional judgment.

Section 16LA repeatedly uses the language of what the relevant person **“considers”**.

The practitioner must consider:

- whether the information is relevant to safeguarding or promoting welfare;
- whether disclosure **may facilitate** the recipient's relevant function;
- and whether disclosure would be more detrimental to the child than non-disclosure.⁴

This is not a mechanical test. Nor does the legislation require the practitioner to establish that disclosure **will** protect the child or that harm is more likely than not.

The phrase **“may facilitate”** deliberately leaves room for preventative action before certainty exists.

That can be essential in safeguarding.

But it also makes professional judgment the principal gatekeeper.

¹⁶ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4.
[Legislation.gov.uk](https://legislation.gov.uk)

That places considerable importance on:

- training;
- supervision;
- accurate recording;
- proportionality;
- challenge;
- and organisational culture.

If practitioners become fearful of being criticised for failing to share, there is a risk that the intended culture of **appropriate sharing** becomes defensive “**share just in case**” practice.

The legislation itself does not authorise indiscriminate sharing. Its wording

“if and only so far as”

the disclosure may facilitate the relevant function points towards limiting disclosure to what is actually required.¹⁷

That limitation needs to remain visible in practice.

6. Consent: what parents can and cannot refuse

This is an area where public discussion can easily become confused.

The new duty does **not** introduce the principle that safeguarding information may sometimes be shared without parental consent. That principle already existed.

The more important change is that, where section 16LA applies, the relevant practitioner has a **statutory duty** to make the disclosure.

DfE's consultation specifically identified confusion around consent, and respondents asked for clearer guidance distinguishing **consent to information-sharing** from **consent to receive a service**. DfE says it strengthened the final guidance accordingly.¹⁸

¹⁷ Children Act 2004, s 16LA(1)–(9), as inserted by Children's Wellbeing and Schools Act 2026, s 4. [Legislation.gov.uk](https://legislation.gov.uk)

¹⁸ Department for Education, *Information sharing duty consultation response*, 10 September 2026. Respondents sought greater clarity on consent, accuracy, transparency, relevance and proportionality, connected adults and SEND; DfE says the final guidance was amended in response. [Consultation Hub](#)

Those are separate questions.

A parent may not be able to stop an appropriate safeguarding disclosure simply by withholding consent.

But that does not automatically mean the family can be compelled to accept every service that follows.

That distinction is particularly important in **Family Help**.

Working Together to Safeguard Children 2026 describes Family Help as a support arrangement bringing together targeted early help and section 17 support within a more integrated model.¹⁹

Where the intervention remains consensual, families can ordinarily decline the service.

That leads to an important principle:

A family can potentially refuse the help while being unable to prevent lawful sharing of the information that led professionals to offer the help.

For parents, that is likely to be one of the most significant practical consequences of the new regime.

How this could work in practice

A school believes a family might benefit from a Family Help assessment.

The parent responds: **“We already have private counselling and support from relatives. We don't want a Family Help assessment.”**

There are two separate issues.

Decision 1: Can the parent decline the service?

Where the support is voluntary, ordinarily yes.

The family should not be compelled to accept a consensual service simply because professionals believe it could be useful.

¹⁹ Department for Education, *Working together to safeguard children 2026*, chapter 3; Family Help brings together targeted early help and section 17 support within a more seamless model

Decision 2: Can the parent prevent the information being shared?

Not necessarily.

If the relevant statutory information-sharing test has been met, the parent's objection does not itself remove the professional's duty.

That produces a potentially delicate situation.

The professional might accurately record: **"Family Help offered. Parent(s) declined because the family already receives private counselling and support from relatives."**

That is very different from: **"Parent(s) refuses support."**

And more different still from: **"Parent(s) has a history of non-engagement."**

The last description contains a judgment that is not necessarily supported by the original facts.

7. Refusing voluntary support should not itself become evidence of risk

This point deserves particular emphasis. The statutory framework does not say:

Refusal of voluntary help = safeguarding concern.

Nor should it be interpreted that way.

Families may decline services for entirely legitimate reasons.

They may:

- already have appropriate support;
- disagree with the proposed intervention;
- have previously had poor experiences with a service;
- believe another service would be more suitable;
- or simply prefer to manage a difficulty without that particular form of professional involvement.

Professionals remain entitled, and where necessary obliged, to assess the underlying circumstances.

If independent evidence gives reasonable cause to suspect significant harm, the fact that the family does not want voluntary support obviously cannot prevent child-protection action.

But those propositions are different. A voluntary service is only meaningfully voluntary if:

declining it does not itself automatically become evidence that the parent presents a safeguarding risk.

This is one of the implementation issues Protect & Teach believes deserves particular attention.

8. What counts as information requiring a response?

The answer is not simply **“anything concerning a child”**.

Section 16LA requires a connection between the information and **safeguarding or promoting welfare**.²⁰

That still leaves considerable room for judgment.

A practitioner might encounter:

Clear risk information

- a disclosure of assault;
- evidence of sexual abuse;
- serious domestic abuse;
- credible exploitation indicators;
- threats of serious violence.

These cases sit close to traditional safeguarding practice.

Emerging concerns

- repeated unexplained absence;
- sudden deterioration in behaviour;
- unexplained injuries;
- contact with known exploiters;
- several weak concerns that collectively create a pattern.

²⁰ Children Act 2004, s 16LA(1)–(9), as inserted by Children’s Wellbeing and Schools Act 2026, s 4.
[Legislation.gov.uk](https://www.legislation.gov.uk)

These cases illustrate the preventive purpose of the new duty.

Wider welfare information

- deteriorating attendance;
- parental difficulty coping;
- unmet SEND needs;
- mental-health difficulties within the family;
- repeated difficulty accessing services;
- concerns about the child's emotional wellbeing.

These cases can still warrant support.

But the further the issue moves from identifiable risk of harm towards a broad conception of welfare, the greater the importance of asking:

Why does this particular information need to be shared with this particular organisation?

That is a better safeguard than treating the label “**welfare**” as sufficient on its own.

9. The first major risk: allegation becoming fact

Safeguarding professionals frequently have to work with uncertain information.

That is unavoidable.

A neighbour, separated parent, relative, another pupil or member of the public may make an allegation.

The allegation may be:

- accurate;
- partly accurate;
- mistaken;
- exaggerated;
- malicious;
- or impossible immediately to verify.

A safeguarding system cannot simply refuse to act until every allegation has been proven.

But the record must preserve what is actually known.

Consider the difference:

Record A

“Mrs X assaulted the child.”

Record B

“On 30 September, Y alleged that Mrs X assaulted the child. The allegation has not been substantiated at this stage.”

Those records convey fundamentally different evidential positions.

If Record B is subsequently summarised as Record A when information moves from school to children's services and then into another system, the problem is not that safeguarding information was shared.

The problem is that **the status of the information changed in transit.**

This is particularly important because DfE's consultation respondents specifically raised the need for stronger guidance around **accuracy**, alongside relevance, proportionality, transparency and information concerning other people connected to the child.²¹

10. Repetition does not equal corroboration

There is another danger once multi-agency sharing becomes more efficient.

Suppose:

- school records an allegation;
- school sends it to social care;
- social care refers to it in a note sent to health;
- health includes it in a summary subsequently viewed by another professional.

Four systems may now contain the same allegation.

But there may still only be **one original source.**

²¹ Department for Education, *Information sharing duty consultation response*, 10 September 2026. Respondents sought greater clarity on consent, accuracy, transparency, relevance and proportionality, connected adults and SEND; DfE says the final guidance was amended in response. [Consultation Hub](#)

That means:

An allegation does not become independently corroborated simply because several agencies now hold copies of it.

A mature information-sharing system therefore needs to preserve **provenance**.

Practitioners need to be able to tell:

- where the information originated;
- who actually observed something;
- what was reported second-hand;
- whether it has been verified;
- whether it has been disputed;
- and what subsequently happened.

The more effectively agencies share information, the more important provenance becomes.

11. Professional opinion is different from fact

This distinction may prove even harder in practice.

Some records involve straightforward facts:

“Child was absent from school on 18 September.”

Others contain professional interpretation:

“Parent(s) appears reluctant to engage.”

Or:

“Family has limited insight into the child's needs.”

Those assessments may sometimes be reasonable and important. But they remain judgments. A later reader may not know the circumstances in which they were made.

For example:

Original event: *Parent declines Family Help because the child already receives private counselling.*

First summary: Parent(s) declined Family Help.

Later summary: The Parent has previously declined support.

Later characterisation: Family has a history of non-engagement with services.

That progression demonstrates how factual compression can gradually produce a substantially different narrative.

The original parent may have been highly engaged with their child's needs throughout.

This is why the lower threshold for early sharing makes accurate contextual recording so important.

12. What happens when information is wrong?

The new information-sharing duty makes **accuracy** more important, not less.

The Information Commissioner's Office states that organisations must take reasonable steps to ensure personal data is accurate, that the **source and status of information is clear**, and that challenges to accuracy are properly considered. It also says records should clearly identify matters of opinion and, where appropriate, whose opinion they are.²²

That matters particularly in safeguarding because records often contain information at different evidential stages.

A case file might include:

- an observed event;
- something reported by a child;
- an allegation made by another adult;

²² Information Commissioner's Office, *Principle (d): Accuracy*. The ICO advises controllers to take reasonable steps to ensure accuracy, make the source and status of information clear, identify matters of opinion and consider challenges to accuracy. [ICO](#)

- a professional opinion;
- a risk assessment;
- an historic concern;
- or a finding reached following investigation.

Those are not interchangeable categories.

An allegation can be accurately recorded even if it later proves unfounded. The accurate fact at the time may simply be that **an allegation was made**.

Likewise, a professional opinion is not necessarily inaccurate because the family disagrees with it. But **it should remain recognisable as an opinion** rather than silently becoming an established fact.

The ICO expressly advises organisations to ensure that the **source and status of personal data is clear** and to distinguish matters of opinion from factual information.²³

That principle is especially important under a regime intended to increase the movement of safeguarding information between organisations.

How this should work in practice: a disputed allegation

A separated parent tells a school: **“My former partner leaves the children unsupervised every night.”**

The school may have legitimate safeguarding reasons to record the allegation and, depending on the circumstances, to share it.

At that point the school does **not necessarily know that the allegation is true**.

A careful record might therefore say:

“On 30 September, Parent A reported that Parent B regularly leaves the children alone overnight. This information has not yet been independently verified.”

²³ Information Commissioner's Office, *Principle (d): Accuracy*. The ICO advises controllers to take reasonable steps to ensure accuracy, make the source and status of information clear, identify matters of opinion and consider challenges to accuracy.

Later investigation establishes that the children were staying with a relative on the dates concerned and **the allegation was inaccurate.**

The original record **should not** simply continue to circulate as:

“History of children being left alone overnight.”

The subsequent finding is part of the accuracy of the record too.

Good record keeping should show:

- what was originally alleged;
- who supplied the information;
- its status at the time;
- what investigation occurred;
- and the eventual outcome.

The aim is not to rewrite history as though the allegation was never made.

It is to ensure that a later professional does not read an **outdated allegation as a current established fact.**

13. Rectification: correcting one record may not be enough

The right to rectification under UK GDPR is an important safeguard.

The ICO says organisations should have systems allowing inaccurate information to be corrected or completed, including through a supplementary statement where appropriate.²⁴

But safeguarding information may already have travelled.

If an organisation rectifies personal data that it previously disclosed to another organisation, Article 19 UK GDPR generally requires it to inform each recipient of the rectification unless doing so is impossible or would involve

²⁴ Information Commissioner's Office, *Right to rectification*; and ICO, *The rights of individuals*, Data Sharing Code of Practice. Where rectified personal data has previously been disclosed, recipients must generally be informed unless this is impossible or involves disproportionate effort; individuals may also ask to be told who those recipients are. [ICO](#)

disproportionate effort. If asked, it must also tell the individual who those recipients were.²⁵

That is potentially a very significant protection.

Consider:

Monday: school records an allegation.

Tuesday: the information is shared with children's social care.

Wednesday: social care passes relevant details to health.

Friday: evidence establishes that a key part of the original information was factually wrong.

Merely amending the school's database does not necessarily prevent the incorrect version continuing to influence decisions elsewhere.

Where the legal rectification requirements apply, the correction needs to **follow the information**.

That leads to an important principle:

The effectiveness of a correction depends upon whether it reaches the places where the incorrect information has already travelled.

The ICO's guidance expressly recognises this problem and requires organisations to have procedures for notifying recipients where data has been rectified.²⁶

²⁵ Information Commissioner's Office, *Right to rectification*; and ICO, *The rights of individuals*, Data Sharing Code of Practice. Where rectified personal data has previously been disclosed, recipients must generally be informed unless this is impossible or involves disproportionate effort; individuals may also ask to be told who those recipients are. [ICO](#)

²⁶ Information Commissioner's Office, *Right to rectification*; and ICO, *The rights of individuals*, Data Sharing Code of Practice. Where rectified personal data has previously been disclosed, recipients must generally be informed unless this is impossible or involves disproportionate effort; individuals may also ask to be told who those recipients are. [ICO](#)

How this could go wrong

Imagine that a school changes: **“Parent regularly leaves child unsupervised”**

To: **“Initial allegation of unsupervised care was investigated and not substantiated.”**

But children's social care still holds the first version.

A subsequent practitioner sees: **“Previous concerns regarding lack of supervision.”**

The family now faces the consequences of information which the originating organisation has already corrected.

This is not primarily a problem with the principle of information-sharing.

It is a **data-governance problem**.

And the more organisations that legitimately receive safeguarding information, the more important that governance becomes.

14. What if the dispute is about professional opinion rather than fact?

This is more difficult.

Suppose a practitioner records:

“In my professional opinion, the parent demonstrated limited understanding of the child's emotional needs.”

The parent may strongly disagree.

That does not necessarily mean the personal data is inaccurate in the GDPR sense.

The record may accurately reflect the fact that **this was the practitioner's opinion at that time**.

The ICO's accuracy guidance recognises this distinction. It says records should clearly identify matters of opinion, whose opinion they are where appropriate, and relevant changes to the underlying facts.²⁷

That means the safeguard is often not simply deletion.

It may instead require:

- **identifying the statement explicitly as professional opinion;**
- **recording the evidence on which it was based;**
- **preserving relevant context;**
- **recording subsequent developments;**
- **and, where appropriate, adding the individual's challenge or supplementary statement.**

This distinction matters because professional judgments can have substantial consequences even where they are not objectively verifiable.

Terms such as:

“limited insight”

“resistant to support”

“failure to engage”

“parent appears controlling”

can influence how subsequent professionals approach a family.

They therefore need to remain traceable to their evidential foundation.

15. A particular danger: factual compression

Multi-agency working often requires information to be summarised.

²⁷ Information Commissioner's Office, *Principle (d): Accuracy*. The ICO advises controllers to take reasonable steps to ensure accuracy, make the source and status of information clear, identify matters of opinion and consider challenges to accuracy. [ICO](#)

That is unavoidable. Professionals cannot always send or read entire case files. But summarisation itself can change meaning.

Consider:

Original note

“The parent declined the Family Help assessment because the child is already seeing a private therapist and the family does not wish to duplicate services.”

First summary: “Family declined Family Help.”

Later summary: “Previous support declined.”

Later assessment: “There has been a pattern of reluctance to engage with services.”

The final statement may convey something substantially different from the original event.

Nothing necessarily involved deliberate falsification. The problem is **progressive loss of context.**

This is especially important where records move through several organisations, each producing its own summary for a different operational purpose.

The new duty therefore makes **context preservation** a safeguarding issue **in its own right.**

16. Different organisations, different operating systems

This is one of the less visible but potentially most important implementation issues.

Schools, GP practices, NHS trusts, police forces, local authorities, youth justice services and other agencies do not necessarily use the same information systems.

The 2026 Act recognises that technical consistency matters.

New section 16LB allows the Secretary of State to prepare **information standards** governing the processing of information for safeguarding and welfare purposes. Organisations to which such standards apply must have regard to them.²⁸

The policy direction is therefore towards greater consistency and potentially greater interoperability.

- That could produce considerable safeguarding benefits.
- Relevant information could be easier to locate.
- Records may be less likely to fall between incompatible systems.
- Patterns may become easier to identify.
- Professionals may spend less time trying to discover which agency holds which part of the picture.

But interoperability has another side.

A system that becomes better at transmitting accurate safeguarding information also becomes better at transmitting inaccurate information if data-quality controls are weak.

The solution is not to avoid interoperability.

It is to ensure that **provenance, corrections, evidential status and context are capable of travelling with the information.**

Four practical interoperability problems

1. Correction mismatch

- A school corrects an inaccurate entry.
- The local-authority database still displays the original version.
- Which version will the next social worker see?

²⁸ Children Act 2004, s 16LB, inserted by Children's Wellbeing and Schools Act 2026, s 4. The Secretary of State may prepare information standards for safeguarding and welfare information, and persons to whom they apply must have regard to them. [Legislation.gov.uk](https://legislation.gov.uk)

2. Loss of evidential status

The original system records: **“Unverified allegation from neighbour.”**

The receiving system has only a short free-text field and records: **“Neighbour reports neglect.”**

A later summary says: **“Concerns regarding neglect.”**

The information has subtly changed at each stage.

3. Different retention periods

- One organisation may conclude that old information no longer needs to be retained.
- Another may continue holding it under a different retention schedule.

That means information which has disappeared from one part of the safeguarding network may continue influencing decisions elsewhere.

4. Duplicate-source illusion

School, GP and social care all appear to have recorded concern about the same parental behaviour.

A later assessor might reasonably think: **“Several agencies have independently raised this.”**

In reality, every entry may trace back to **one telephone call made by one person.**

This is why identifying the **original source** matters.

17. The new system needs provenance, not just connectivity

“Who said what, and on what basis?” is one of the most important safeguarding questions in any multi-agency record. The status of information should remain visible.

Professionals should be able to distinguish:

Observed:

"I saw bruising on the child's upper arm."

Reported by child:

"The child said X struck them."

Third-party allegation:

"The neighbour alleges that X struck the child."

Professional interpretation:

"In my view, the explanation given is inconsistent with the injury."

Subsequent finding:

"Police investigation resulted in..."

These may all be relevant. **But they are evidentially different.**

A high-quality safeguarding system should preserve that distinction rather than flatten everything into a generic category of **"concerns"**.

The Government's intention to improve information-sharing therefore needs to be matched by equally strong standards around **information lineage and quality**.

18. Information about parents and other adults

The scope of section 16LA is wider than information directly about a child.

It applies where the relevant person holds:

information about the child **or information about another individual that relates to the child.**²⁹

²⁹ Children Act 2004, s 16LA(1)–(2), inserted by Children's Wellbeing and Schools Act 2026, s 4. The duty includes information about another individual relating to the child, subject to the relevance and disclosure tests. [Legislation.gov.uk](https://legislation.gov.uk)

There are obvious circumstances where that is necessary.

Information about a parent or another adult may be directly relevant where there is:

- domestic abuse;
- serious substance misuse;
- violent offending;
- exploitation;
- coercive control;
- or another identifiable risk to the child.

But the provision is not limited to those examples.

This raises an important privacy question:

How much information about an adult is genuinely necessary to share in order to safeguard or promote the welfare of the child?

The existence of information about the parent is not by itself sufficient.

The statute still requires relevance to the child and requires disclosure only **“if and only so far as”** the professional considers it may facilitate the recipient's relevant functions.³⁰

That wording should operate as a limiting principle.

How this should work: a parent's health information

A parent tells their GP that they are experiencing severe depression.

The fact that somebody is experiencing a mental-health difficulty does not by itself establish that their child is unsafe or inadequately cared for.

³⁰ Children Act 2004, s 16LA(1)–(2), inserted by Children's Wellbeing and Schools Act 2026, s 4. The duty includes information about another individual relating to the child, subject to the relevance and disclosure tests. [Legislation.gov.uk](https://legislation.gov.uk)

Suppose, however, the parent also explains that their condition has deteriorated to the point that they are repeatedly unable to collect a young child from school or provide essential care.

Some information may then become directly relevant to the child's welfare.

But there remains an important distinction between:

sharing the minimum information necessary to explain the child's welfare concern

and

sharing the parent's entire medical history.

The new duty does not abolish data minimisation or proportionality.

The question should remain:

What does this recipient genuinely need to know in order to perform the relevant safeguarding or welfare function?

19. Could families become less willing to ask for help?

This is a possible unintended consequence which deserves monitoring.

Early-help policy relies partly on families being willing to tell professionals when they are struggling.

A parent may disclose:

- financial difficulty;
- mental-health problems;
- relationship breakdown;
- difficulty managing a child's SEND needs;
- problems with attendance;
- or concern about their own capacity to cope.

Those disclosures can enable valuable support.

But if families come to believe that discussing difficulty automatically results in information moving around a broad safeguarding network, some may become more cautious about asking for help.

There is not yet evidence that the new statutory duty **will** produce that effect.

It would therefore be wrong to present it as an established consequence.

But it is a plausible implementation risk because the Government's wider social-care reforms explicitly aim to shift provision away from crisis intervention and towards **earlier support and prevention**.³¹

A system intended to encourage earlier help would be undermined if families became less willing to disclose emerging problems.

That makes transparency especially important.

20. Transparency is not the same as consent

Professionals should be careful not to confuse these ideas.

A family does not necessarily have to **consent** to lawful sharing under section 16LA. But wherever it is safe and appropriate, they should still understand:

- what information is being used;
- why it is being shared;
- who may receive it;
- and what rights they have concerning their data.

Transparency serves a different purpose from consent.

It enables scrutiny. It also enables families to identify mistakes before those mistakes become embedded across several systems.

³¹ Department for Education, *Supporting local areas to embed Working Together to Safeguard Children and the National Framework*, updated 18 March 2026. DfE describes the reforms as seeking to rebalance children's social care away from crisis intervention towards prevention and earlier support. [GOV.UK](https://www.gov.uk)

Where disclosure to a parent would itself increase risk to the child, undermine an investigation or create some other safeguarding danger, different considerations obviously apply.

But outside such circumstances, secrecy should not become the default merely because parental consent is no longer the legal gateway.

21. Privacy and family life: does Article 8 matter?

Yes. Article 8 of the European Convention on Human Rights protects the right to respect for **private and family life, home and correspondence**. In the UK, public authorities must act compatibly with Convention rights unless primary legislation requires otherwise.

Article 8 is not absolute. Interference can be lawful where it is:

- in accordance with the law;
- directed towards a legitimate aim;
- and necessary and proportionate.

Safeguarding children is plainly capable of amounting to a legitimate aim.

The existence of section 16LA also provides a clear statutory basis for information-sharing where its conditions are met.

But that does not make proportionality irrelevant.

A lawful statutory power still has to be exercised within its proper scope.

That means the rights question is not:

“Can safeguarding information ever be shared without consent?”

It plainly can.

The better question is:

“Was this particular interference with privacy justified by the safeguarding or welfare purpose being pursued, and was no more information shared than was reasonably required?”

That distinction becomes especially important at the **lower end of the new threshold**, where the concern may involve early help or general welfare rather than suspected significant harm.

The broader the concept of welfare being relied upon, the more important it becomes to explain why a particular disclosure was relevant and proportionate.

The ICO likewise says that children's information requires particular care and that sharing should have a compelling justification, taking the child's best interests into account.³²

How proportionality could look in practice

Scenario A: proportionate

A GP knows that a parent has deteriorated to the point that they are repeatedly unable to care safely for a very young child.

Sharing the relevant information with children's services may be justified.

That does not necessarily mean disclosing the parent's **entire medical record**.

The relevant information may instead be limited to what explains:

- the current difficulty;
- the resulting impact on the child;
- and any immediate risk or support needed.

Scenario B: potentially disproportionate

- A parent once received counselling for anxiety five years earlier.
- A school now has an unrelated attendance concern about the child.

The mere existence of historic mental-health information should not automatically make that material relevant to the current welfare issue.

³² Information Commissioner's Office, *Can we share children's personal information?* and *Data sharing and children*. The ICO says organisations must take particular care with children's information, have a compelling reason for sharing, consider the child's best interests and address risks arising from disclosure. [ICO](#)

The statutory question is still whether the information relates to safeguarding or promoting **this child's welfare**, and whether sharing it may facilitate the recipient's relevant function.³³

That is where proportionality should prevent "just in case" accumulation of sensitive information.

22. Confidentiality has changed, but it has not disappeared

One of the stronger effects of the new law is on **professional confidentiality**.

New section 16LA provides that a disclosure under the section does not breach an obligation of confidence owed by the person making it.

The explanatory notes make clear that this includes the common-law duty of confidentiality between a patient and a healthcare professional.³⁴

That is a substantial legal protection for practitioners.

A GP, nurse, teacher or other professional should not be prevented from making a disclosure required by section 16LA merely because the information was originally provided in confidence.

But that does not mean: **"Confidential information is now freely shareable."**

The statutory conditions still have to be met.

And data-protection law continues to apply. So confidentiality is displaced **for the particular lawful disclosure**, not abolished as a general principle.

That matters because trust remains a central part of effective safeguarding.

³³ Children Act 2004, s 16LA(1)–(3), inserted by Children's Wellbeing and Schools Act 2026, s 4. The statutory test concerns relevance to safeguarding or promoting welfare, whether disclosure may facilitate a recipient's relevant function, and the more-detrimental exception. [Legislation.gov.uk](https://legislation.gov.uk)

³⁴ Children's Wellbeing and Schools Act 2026, Explanatory Notes, paras 154–163. Paragraph 161 explains that s 16LA(7) prevents disclosure under the section from breaching an obligation of confidence, expressly including common-law confidentiality between patients and healthcare professionals. [Legislation.gov.uk](https://legislation.gov.uk)

- A parent who tells a GP they are struggling should not reasonably assume every detail will automatically circulate across local services.
- Equally, a professional should not promise absolute secrecy where information may need to be shared to protect or support a child.

A better approach is openness about those boundaries from the outset.

23. The “more detrimental” exception: an important but narrow safeguard

Section 16LA contains a significant exception.

The duty to disclose does not apply if the relevant person considers that disclosure would be **more detrimental to the child than not disclosing it**.³⁵

That creates a child-centred safeguard.

It recognises that information-sharing itself can sometimes create danger.

Examples might include circumstances where disclosure could:

- reveal the location of a child or protective parent to an alleged abuser;
- expose a child to retaliation;
- compromise an active investigation;
- disclose highly sensitive information in a way likely to cause serious harm;
- or otherwise increase the child’s risk.

The important word is **child**.

The test is not whether sharing would be inconvenient, embarrassing or unwelcome to an adult.

Nor is it simply whether the parent objects.

³⁵ Children Act 2004, s 16LA(3), inserted by Children’s Wellbeing and Schools Act 2026, s 4.
[Legislation.gov.uk](https://legislation.gov.uk)

The practitioner must consider whether disclosure would be **more detrimental to the child** than withholding it.

That prevents the exception becoming a general parental veto. But it also creates another area of significant professional discretion.

Two practitioners could conceivably assess the same potential detriment differently.

That is why the decision and reasoning should be clearly recorded.

How this could work

- A mother and child are living at a confidential address after fleeing serious domestic abuse.
- A professional holds information about the child's current location.
- Another service requests information because it is involved in the child's welfare.

The professional should not automatically send the child's address merely because the requesting organisation is within the safeguarding network.

If disclosure of the address could expose the family to danger, the **detriment exception and data-minimisation principles** become highly relevant.

The organisation may be able to share the welfare information needed without sharing the protected location.

This is an example of why good safeguarding sometimes requires **sharing less**, not more.

24. More lawful sharing also creates more security responsibility

The new duty **does not suspend data-security obligations.**

The ICO states that organisations must put appropriate technical and organisational measures in place, protect information against

unauthorised or unlawful processing and accidental loss, and consider the risks inherent in transfers between organisations.³⁶

That becomes particularly important when highly sensitive information is moving between:

- schools;
- GP systems;
- NHS trusts;
- local authorities;
- police;
- early-help services;
- and other safeguarding partners.

There is an obvious safeguarding advantage to information reaching the right professional quickly.

But every additional transfer also creates another point at which information can potentially be:

- sent to the wrong recipient;
- accessed inappropriately;
- copied unnecessarily;
- retained beyond need;
- misclassified;
- or exposed through a cyber incident.

This does **not** mean the new duty will necessarily cause more data breaches.

That would go beyond the evidence.

But increasing legitimate data movement logically increases the importance of strong security controls.

The ICO itself says sharing children's information with third parties can expose them to unintended risks if not handled properly, and recommends

³⁶ Information Commissioner's Office, *Sharing data to safeguard children FAQs*. The ICO states that organisations must use appropriate technical and organisational measures, comply with the UK GDPR security principle and assess appropriate methods for secure transfer. [ICO](#)

risk assessment and, where required, Data Protection Impact Assessments.³⁷

What happens if there is a breach?

Organisations have continuing duties under UK GDPR.

Where a personal-data breach is likely to pose a risk to individuals' rights and freedoms, the organisation must generally notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it.

Where the breach is likely to result in a **high risk**, affected individuals must also generally be informed without undue delay.³⁸

Safeguarding information can be especially sensitive.

A breach might expose:

- abuse allegations;
- health information;
- domestic-abuse information;
- a protected address;
- details of children in care;
- information about family relationships;
- or police intelligence.

The consequences could therefore extend beyond privacy embarrassment and into **actual safeguarding risk**.

That makes cybersecurity part of the safeguarding framework, not a separate technical issue.

³⁷ Information Commissioner's Office, *Can we share children's personal information?* and *Data sharing and children*. The ICO identifies unintended risks from third-party sharing and the role of Data Protection Impact Assessments in identifying and mitigating high-risk processing. [ICO](#)

³⁸ Information Commissioner's Office, *UK GDPR data breach reporting* and *Personal data breaches: a guide*. Organisations must assess risk following a personal-data breach; qualifying breaches must generally be reported to the ICO within 72 hours where feasible, and high-risk breaches normally require notification of affected individuals without undue delay. [ICO](#)

25. Retention: how long can early concerns follow a family?

This is another area where the practical effect may differ between agencies.

UK data-protection law does not impose one universal retention period for all safeguarding records.

The ICO's position is that organisations should retain personal data only for as long as they need it for the purpose for which it is being processed, and should be able to justify and document that period.³⁹

Different organisations may nevertheless have legitimate reasons for applying different retention schedules.

That creates a practical difficulty.

- An early-help concern may be closed by one service but remain visible elsewhere.
- An allegation may have been investigated and found unsupported but still appear within an older record.
- A professional several years later may encounter historic material without understanding how it was resolved.

This does not mean historical information should always be deleted.

Safeguarding sometimes depends on identifying patterns over time.

But there is an important difference between preserving **accurate historical information with its outcome** and preserving an unresolved adverse label indefinitely.

The key question is:

Does the record still explain what happened, or does it merely preserve the original concern?

³⁹ Information Commissioner's Office, *Sharing data to safeguard children FAQs*, question 2. The ICO states that there is no universal data-protection retention period: personal data should be kept only for as long as necessary and organisations should justify and document retention. [ICO](#)

26. What can parents actually ask to see or correct?

Parents and children retain data-protection rights, although those rights are not absolute in safeguarding circumstances.

The ICO says organisations should have arrangements enabling individuals to exercise rights including:

- subject access;
- rectification;
- erasure where applicable;
- restriction;
- objection;
- and certain rights concerning automated decision-making.

But safeguarding exemptions may limit disclosure or other rights where exercising them would itself create serious risk, for example, where revealing information would be likely to cause serious harm to a child.⁴⁰

So a parent cannot assume:

“I have a GDPR right, therefore the organisation must immediately give me everything.”

But neither should safeguarding be used as a blanket reason to refuse legitimate questions.

Where appropriate, a parent could reasonably ask:

- What information do you hold about me or my child?
- What is the source of that information?
- Is it recorded as fact, allegation or professional opinion?
- Who has received it?
- What lawful basis are you relying on?
- Has it been corrected or updated?
- If it was shared before correction, were recipients informed?
- How long will it be retained?

⁴⁰ Information Commissioner's Office, *A 10 step guide to sharing information to safeguard children*, step 4. Organisations should facilitate individual information rights, while recognising that safeguarding circumstances can restrict some rights, including where disclosure would be likely to cause serious harm to a child.

- What is the route for challenging an inaccurate record?

Those questions are entirely compatible with safeguarding.

Indeed, they can improve data quality.

Worked example: the parent discovers an old allegation

A parent makes a subject-access request and discovers the following entry:

“Concern that mother frequently leaves child unattended.”

The parent says this originated from a malicious allegation made during a family dispute and was investigated two years earlier.

The useful next questions are not simply: **“Can I have this deleted?”**

They are:

1. **What was the original source?**
2. **Was the allegation investigated?**
3. **What was the outcome?**
4. **Does the current record show that outcome?**
5. **Has the allegation been presented elsewhere as an established fact?**
6. **Which organisations received it?**
7. **If the data is inaccurate, will those recipients be notified of the correction?**

That is a much more effective challenge than treating all disputed safeguarding information as something that should simply disappear.

27. What if the family still disagrees?

There are several potential routes, depending on the issue.

- If the problem concerns **record accuracy**, the family can raise it with the organisation responsible for the data and its Data Protection Officer.

- If the dispute concerns **how personal information has been processed**, the individual may complain to the ICO.
- If the issue concerns professional practice or the substance of a safeguarding decision, the relevant organisation's complaints or safeguarding-review procedures may be more appropriate.
- Local authorities and safeguarding bodies may also have their own complaints and escalation processes.
- In rare cases involving serious disputes about legality, proportionality or public-authority decision-making, court proceedings may be available.

The important point is that different complaints mechanisms address **different questions**.

For example:

- **"That factual entry is wrong"** is principally a data-quality issue.
- **"I disagree with the social worker's professional assessment"** is not necessarily the same thing.
- And: **"The council had no lawful basis for sharing this information at all"** raises a different legal question again.

Parents and professionals need to distinguish those categories if challenges are to be dealt with properly.

28. Does the framework contain enough safeguards?

At this point, the picture is more balanced than either extreme suggests.

The new duty is **not** a general licence to circulate family information.

The law contains limiting features:

- information must be relevant to safeguarding or promoting welfare;
- sharing must be capable of facilitating a recipient's relevant function;
- disclosure is limited by the wording **"if and only so far as"**;
- the more-detrimental-to-the-child exception applies;
- data-protection obligations remain;
- children's information attracts particular care;
- transparency and individual rights remain relevant;

- organisations have duties concerning accuracy, retention and security;
- and statutory guidance must be taken into account.^{41 42 43}

Those are meaningful safeguards.

But the framework also gives professionals **substantial discretion**.

The operative concepts include:

- **“relevant”;**
- **“promoting welfare”;**
- **“may facilitate”;**
- **and “more detrimental”.**

Those are deliberately judgment-based concepts.

That is understandable in safeguarding because children's circumstances cannot be reduced to a rigid checklist.

But it means much of the practical balance will depend upon **how organisations train staff and how individual professionals exercise judgment**.

29. Where Protect & Teach thinks the balance needs watching

The most important risk is not simply excessive sharing.

It is the interaction between **a broad statutory threshold and imperfect real-world information systems**.

That produces several particular areas for scrutiny.

⁴¹ Children Act 2004, s 16LA(1)–(3), inserted by Children’s Wellbeing and Schools Act 2026, s 4. The statutory test concerns relevance to safeguarding or promoting welfare, whether disclosure may facilitate a recipient’s relevant function, and the more-detrimental exception. [Legislation.gov.uk](https://legislation.gov.uk)

⁴² Information Commissioner’s Office, *Can we share children’s personal information?* and *Data sharing and children*. The ICO identifies unintended risks from third-party sharing and the role of Data Protection Impact Assessments in identifying and mitigating high-risk processing. [ICO](https://ico.org.uk)

⁴³ Information Commissioner’s Office, *A 10 step guide to sharing information to safeguard children*, step 4. Organisations should facilitate individual information rights, while recognising that safeguarding circumstances can restrict some rights, including where disclosure would be likely to cause serious harm to a child.

1. Early welfare concerns

- The duty extends below significant harm.
- That may facilitate earlier support, but professionals must continue distinguishing genuine welfare relevance from information that is merely interesting, sensitive or potentially useful.

2. Unverified allegations

- Sharing may sometimes be justified before an allegation is proven.
- But its unverified status and original source should follow it.

3. Professional opinions

- Professional judgment is unavoidable.
- But opinion should not silently acquire the status of fact as it passes between organisations.

4. Voluntary support

- A family may decline voluntary Family Help.
- Declining one form of support should not itself be transformed into evidence of safeguarding failure without a separate evidential basis.

5. Connected adults

- Relevant information about parents and other adults may legitimately be shared.
- That does not justify circulating their entire personal history.

6. Multi-agency systems

- Improved connectivity can strengthen safeguarding.
- It can also distribute mistakes more efficiently.

7. Correction

- A meaningful rectification system must address information that has already travelled, not merely the originating record.

8. Retention

- Historic concerns may be relevant to pattern recognition, but they should retain their context and outcome rather than becoming permanent unexplained adverse markers.

9. Security

- More lawful information-sharing makes access controls, transfer security, audit logs and breach procedures more important.

10. Trust

- Early intervention depends partly upon families being willing to speak candidly with professionals.
- If families perceive every disclosure of difficulty as potentially entering a broad safeguarding network, that could undermine the very early-help objective the reforms seek to promote.

That final point is a risk to monitor, rather than an established consequence.

30. The balance: child protection and family rights are not opposites

It would be a mistake to frame this reform as a simple contest between:

protecting children and **protecting parental rights**.

- Children need adults and organisations to share information when serious risks would otherwise remain hidden.
- They also need safeguarding systems that are accurate, proportionate, secure and capable of correcting errors.
- Parents do not have an absolute right to prevent safeguarding information being shared.

But nor should involvement with children's services extinguish legitimate expectations of privacy, accuracy, transparency and fair treatment.

Those principles reinforce good safeguarding rather than obstructing it.

A system that withholds genuinely important information can fail a child.

A system that circulates inaccurate, irrelevant or decontextualised information can also fail a child.

The policy objective should therefore be neither **maximum secrecy** nor **maximum sharing**.

It should be:

the right information, shared with the right person, for a clear safeguarding or welfare purpose, at the right time, with its source, context and evidential status preserved.

That is the standard against which implementation of section 16LA should ultimately be judged.

Protect & Teach: what we will be watching

Implementation: whether “promoting welfare” is being applied proportionately.

Voluntariness: whether declining Family Help remains genuinely voluntary in practice.

Data quality: whether systems preserve fact, allegation, professional opinion and provenance.

Correction: whether rectifications actually propagate between agencies.

Trust and unintended consequences: whether the new regime helps families seek support earlier or makes some families more reluctant to disclose difficulties.

Protect & Teach will keep implementation of the new information-sharing duty under review as practice develops.

References

Children Act 2004, ss 16LA–16LB, as inserted by Children’s Wellbeing and Schools Act 2026, s 4. Available at: [legislation.gov.uk](https://www.legislation.gov.uk).

Available online: <https://www.legislation.gov.uk/ukpga/2026/21/section/4>

Children’s Wellbeing and Schools Act 2026, s 4.

Available online: <https://www.legislation.gov.uk/ukpga/2026/21/section/4>

Children’s Wellbeing and Schools Act 2026, Explanatory Notes, paras 154–163.

Available online:

https://www.legislation.gov.uk/ukpga/2026/21/pdfs/ukpgaen_20260021_en.pdf

Children’s Wellbeing and Schools Act 2026 (Commencement No. 2) (England) Regulations 2026, SI 2026/803, reg 6.

Available online: <https://www.legislation.gov.uk/uksi/2026/803>

(Reg 6(a) brings s 4 into force on 30 September 2026 only so far as it inserts Children Act 2004, ss 16LA and 16LB.)

Department for Education, *Information sharing duty consultation response*, 10 September 2026.

Available online: <https://consult.education.gov.uk/mais-strategy-policy-and-programme-unit/statutory-guidance-for-information-sharing-duty/>

Department for Education, *Information sharing to safeguard children and young people* (statutory guidance), updated 10 September 2026.

Available online: <https://www.gov.uk/government/publications/information-sharing-to-safeguard-children-and-young-people>

Department for Education, *Supporting local areas to embed Working Together to Safeguard Children and the National Framework*, updated 18 March 2026.

Available online: <https://www.gov.uk/government/publications/improving-practice-with-children-young-people-and-families/supporting-local-areas-to-embed-working-together-to-safeguard-children-and-the-national-framework--2>

Department for Education, *Working together to safeguard children 2026* (statutory guidance), updated 18 March 2026.

Available online: <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Department for Education, *Working together to safeguard children 2026: summary of changes*, 18 March 2026.

Available online: <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2/working-together-to-safeguard-children-2026-summary-of-changes>

Information Commissioner's Office, *A 10 step guide to sharing information to safeguard children*.

Available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children>

Information Commissioner's Office, *Can we share children's personal information?*

Available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/can-we-share-children-s-personal-information/>

Information Commissioner's Office, *Data sharing and children*.

Available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-and-children/>

Information Commissioner's Office, *Personal data breaches: a guide*.

Available online: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide>

Information Commissioner's Office, *Principle (d): Accuracy*.

Available online: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>

Information Commissioner's Office, *Right to rectification*.

Available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/>

Information Commissioner's Office, *Sharing data to safeguard children FAQs*.

Available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-data-to-safeguard-children-faqs/>

Information Commissioner's Office, *The rights of individuals* (Data Sharing Code of Practice).

Available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/the-rights-of-individuals/>

ICO guidance cited was current at the date of publication; several ICO pages note that guidance is under review following the Data (Use and Access) Act.