Consultation response form

Please complete this form in full and return to DCUguidance@ofcom.org.uk

Consultation title	Consultation: Deceased Child User Duties
Full name	Dr Edina Harbinja, Associate Professor in Law
Contact phone number	
Representing (delete as appropriate)	Self
Organisation name	University of Birmingham, Birmingham Law School
Email address	

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None
For confidential responses, can Ofcom publish a reference to the contents of your response?	Yes

Your response

Question	Your response
Question 1: Do you agree with our proposed objectives for the Guidance? Please explain why.	Confidential? N The proposed objectives for the Guidance—to increase transparency, reduce uncertainty, and lower barriers for bereaved parents—are commendable in their focus on the "relational-living" interests of families. Transparency is vital for parents attempting to understand the circumstances surrounding a child's death, particularly in cases involving online harm, such as those highlighted by the Molly Russell inquest. However, from a postmortem privacy perspective, these objectives are incomplete if they do not explicitly incorporate the protection of the deceased child's dignity and the privacy of third parties. Transparency should not be a synonym for "unfiltered access" to a child's digital life; rather, it should signify clarity in the *process* of disclosure and the *rationale* behind what is or is not shared. My research highlights that the "best interests of the child" principle does not terminate at death. Therefore, the Guidance objectives should be expanded to include the objective of ensuring that any disclosure is "proportionate" and "necessary." A purely parent-centric objective risks commodifying the child's digital persona and ignoring the child's autonomous right to a "private life" that may have included secrets kept even from their parents. By including the protection of the deceased child's dignity as a core objective, Ofcom can ensure that service providers adopt a "trauma-informed" approach that respects both the

Question	Your response
	grieving family and the individual who has passed. Furthermore, the objective of "reducing uncertainty" must apply equally to children who are currently using these services. Although not child-specific, my empirical studies suggest that users value postmortem privacy and wish to maintain control over their digital remains.[1] If the Guidance focuses solely on the ease of parental access, it may create a "chilling effect" on the freedom of expression for living children, who may fear that their private correspondences will be exposed to their parents upon their death. Thus, the Guidance should aim to strike a delicate balance that provides parents with the answers they need for closure while maintaining the integrity and dignity of the child's digital self.
Question 2 a): In relation to each of the following areas, do you agree with our proposals? Please tell us why: i) A provider of a relevant service's policy about disclosure of information; ii) The procedure for parents to make a request; iii) The evidence the provider will require; iv) Sufficient detail about the disclosure of information.	Confidential? – N The proposal to require providers to specify their disclosure policy in their terms of service is a necessary step toward resolving the "posthumous privacy paradox" by managing expectations before a tragedy occurs. However, the Guidance must require providers to adopt a "restrictive interpretation" of the phrase "information about the child's use of the service". A disclosure policy should not be a blanket statement of cooperation; it must detail the *categories* of data that are eligible for disclosure and those that are strictly protected. For example, general usage logs (time spent,

[1] https://www.tandfonline.com/doi/full/10.1080/13600869.2025.2506164

Question	Your response
	login frequency) carry a lower privacy weight than the content of private messages, which involves the privacy of third parties. Regarding the procedure and evidence requirements, the emphasis on clarity and accessibility is vital to avoid compounding the "administrative trauma" of bereaved parents. My research indicates that individuals, including parents, often face significant barriers, such as being ignored by service providers or facing complex legal hurdles. The proposal to accept varied forms of evidence beyond government-issued IDs—such as parental responsibility documentation or local authority letters—is a positive step toward inclusivity and recognises the diversity of family structures. However, the procedure should also include a "verification of necessity" step, where parents are asked to specify the *purpose* of their request, allowing providers to tailor the disclosure to the specific need for answers while redacting non-essential, sensitive data. The requirement for "sufficient detail" about what will be shared is crucial for both parents and children to be "reasonably certain" of the outcomes. From a postmortem privacy lens, this detail must include an explanation of the *redaction process*. If a provider's policy is to redact third-party identifiers or delete intimate media files that do not pertain to the parent's inquiry, this should be clearly stated. This prevents parents from feeling misled and ensures that the child's "informational body" is not subjected to unnecessary postmortem "autopsy" by the platform or the family.
Question 2 b): In relation to the provisions in Question 2(a), are there	Confidential? – N

Question	Your response
other examples of good practice we should consider?	Good disclosure practice should revolve around the concepts of "granular control" and "pre-mortem autonomy". Service providers should be encouraged to implement tools during the child's life—similar to Apple's Legacy Contact or Facebook's Legacy Contact—that allow the child to nominate who should have access to their data and what *types* of data should be shared. While the Act focuses on the postmortem request by parents, the most effective way to respect a child's dignity is to honour their ante-mortem wishes. Providers should actively promote these tools to children in an age-appropriate way, framing them as a component of digital self-determination rather than just "death planning". Another critical good practice is implementing "manual screening and redaction" for sensitive data requests. Automated data-dump tools are often inappropriate in the context of bereavement, as they may expose third-party data or intimate content that is irrelevant to the parents' specific concerns about their child's safety. Providers should offer a "curated archive" or a "redacted summary" as the primary method of disclosure, ensuring that the privacy of the child's friends and contacts—who may also be minors—is preserved. This "privacy-by-design" approach to disclosure aligns with the broader goals of the Online Safety Act to protect all children on the service. Furthermore, good practice should involve "transparency about what is NOT shared". Providers should give parents a clear rationale for withholding certain data, perhaps citing the specific privacy rights of third parties or the child's stated preferences. This reduces the suspicion that platforms are "covering up"

Question	Your response
	evidence and fosters a more collaborative relationship between the service and the bereaved family. Finally, providers should offer "secure delivery mechanisms" for the disclosed data, ensuring that sensitive information does not fall into the wrong hands and that the child's digital remains are handled with the same security as their medical records
Question 3 a): Do you agree with our proposals regarding providers responding in a timely manner? Provide any evidence to support your answer.	Confidential? – N The requirement for providers to respond in a "timely manner" is of paramount importance, as the delay in receiving information can significantly hinder the grieving process and legal investigations. Research highlights that many parents currently face a "battle" for transparency that can last months or even years. However, "timely" must be defined with sufficient specificity to be enforceable yet flexible enough to accommodate the complex redaction processes required to protect postmortem privacy. The Guidance should suggest a benchmark of 20 working days for an initial substantive response, aligning with the standards set by the Freedom of Information Act or the GDPR's Subject Access Request window of one calendar month. Proactive communication is essential during this timeframe. Providers should be required to send an immediate acknowledgement of the request and provide regular updates (e.g., every 10 days) on the progress of the data review. This reduces the sense of abandonment many parents feel when dealing with large technology firms. From a postmortem dignity perspective, "timeliness" also includes the "prompt deletion" of data if that was the child's wish, or the "prompt memorialisation"

Question	Your response
	of the account to prevent further interactions that might distress the family. The speed of the response must match the sensitivity of the communication. However, the "timely manner" duty must not lead to "reckless disclosure". Providers must not be pressured into skipping the necessary legal and ethical checks to protect the privacy of the deceased and third parties just to meet a deadline. The Guidance should clarify that a "timely response" includes providing a detailed explanation when the disclosure process is delayed due to complex privacy considerations, such as consulting legal teams or redacting vast amounts of third-party data. This balanced approach ensures that speed does not come at the expense of dignity.
Question 3 b): Are there other examples of good practice we should consider?	Confidential? – N Good practice should include "priority flagging" for requests related to active coronial or police investigations. While the deceased child user duties are independent of coronial powers, providers should synchronise their workflows to ensure that parents receive relevant information in a timeframe that supports the legal determination of the cause of death. This "joined-up" approach between the platform, the regulator, and the legal system is essential for providing families with the closure they seek. Additionally, providers should consider "staged disclosure" as a method for maintaining timeliness. Basic information that requires minimal redaction—such as account creation dates, general login history, or public posts—could be disclosed quickly, while more sensitive and correspondence-heavy data follows

<table>
<tr><th>Question</th><th>Your response</th></tr>
<tr><td></td><td>after a more thorough review. This provides parents with immediate progress while maintaining the rigorous standards required for protecting postmortem privacy.

Finally, good practice should involve "performance transparency". Providers, particularly those providing Category 1 services, should be encouraged to publish their average response times for deceased-child user requests in their transparency reports. This public accountability mechanism incentivises companies to invest in the specialised staff and infrastructure needed to handle these requests efficiently and sensitively. By benchmarking response times, Ofcom can identify services that are failing to treat bereaved parents with the "respect and sensitivity" required by the Act.

Table 2: Recommended Benchmarks for Timely Responses
<table><tr><th>Action</th><th>Recommended Timeframe</th><th>Rationale</th></tr><tr><td>Acknowledgment</td><td>Within 48 Hours</td><td>To reduce parental anxiety and confirm receipt of request.</td></tr><tr><td>Initial Update</td><td>Within 10 Working Days</td><td>To inform parents of the complexity and expected delivery date.</td></tr><tr><td>Substantive Response</td><td>20–30 Calendar Days</td><td>Aligns with GDPR/FOI standards for complex data requests.</td></tr></table></td></tr>
</table>

Question	Your response
	<table><tr><td>Complex Extension</td><td>Up to 60 Additional Days</td><td>Necessary for manual redaction of high-volume private content.</td></tr><tr><td>Appeal/Complaint Resolution</td><td>Within 15 Working Days</td><td>Rapid redress for procedural failures is essential for grieving families.</td></tr></table>
Question 4: Do you agree with our proposal to require providers of relevant services to also make their disclosure policy statement accessible as well as clear? Please explain why.	Confidential? – N The proposal to require disclosure policies to be "accessible" as well as "clear" is fundamental to a "trauma-informed" regulatory approach. For a parent in the depths of grief, a standard, jargon-heavy "Terms of Service" document is virtually impenetrable. Accessibility must therefore be understood as "cognitive accessibility"—the policy must be written in plain, empathetic language that avoids technical terms like "data controller," "fiduciary access," or "interoperability". The policy should be designed as a "safety resource" rather than a legal disclaimer, clearly outlining the steps a parent needs to take without requiring them to decipher complex corporate policy. From the perspective of postmortem dignity, "accessibility" also means that the policy must be easy to *find* without the parent having to log into the deceased child's account. Policies should be prominently featured in the service's "Safety Centre" or on a dedicated "Bereavement Support" page. For search services (Category 2A), where a user might not have a direct account relationship with the provider, these statements must be easily discoverable through a simple search for "deceased user policy" or "parental access after death". This

Question	Your response
	reduces the burden on parents who are already struggling with the cognitive load of trauma. Furthermore, the policy should be available in "multiple formats" to ensure it reaches all demographics. Good practice would include the provision of short video explainers or audio summaries that walk parents through the request process. For children using the service, the policy should also be summarised in age-appropriate language, ensuring they understand the conditions under which their data might be shared with their parents after their death. This transparent approach respects the child's autonomy and helps them make informed decisions about their digital footprint while they are still alive.
Question 5: Do you have any comments in relation to our proposal to align our approach to clarity and accessibility with the approaches taken in our Illegal Harms and Protection of Children Codes? Please explain why.	Confidential? – N Aligning the approach to clarity and accessibility with the Illegal Content and Protection of Children Codes is a logical and efficient strategy. These codes already establish high standards for user-centric design and reading-age appropriateness, which are highly relevant to the "Deceased Child User Duties". Since many bereaved parents may also be interacting with the platform's "user reporting" systems—perhaps reporting the very content that they believe harmed their child—having a consistent design language and terminology across these different safety functions is essential. It prevents the parent from having to learn multiple administrative systems during a crisis. However, the "Deceased Child User Duties" represent a unique intersection of safety, privacy, and succession law that the general safety codes do not fully address. While the

Question	Your response
	interface should be aligned, the *substance* of the guidance must remain distinct. For example, "illegal content" is often handled via automated hashes and rapid removal, whereas "postmortem data disclosure" requires a nuanced, human-led balancing of competing privacy interests. Ofcom must ensure that alignment does not lead to the "automation" of bereavement requests. The specialised nature of postmortem dignity requires a more "bespoke" approach than the high-volume moderation of illegal content. Moreover, the "Protection of Children" code focuses on preventing harm to *living* children, whereas Section 75 focuses on the interests of the *relational-living* (the parents) and the *deceased* child. My research suggests that while these goals are related, they can sometimes conflict. For instance, a safety measure that automatically shares a living child's data with parents for "protection" might violate that same child's "postmortem privacy" expectations if they die. Therefore, the alignment should prioritise a unified "trauma-informed" design philosophy while maintaining the specific legal and ethical safeguards required for digital remains.
Question 6: Are there other examples of good practice in relation to clarity and accessibility we should consider?	Confidential? – N A primary good practice for clarity and accessibility is the use of "visual procedural aids". Providers should offer flowcharts or interactive step-by-step guides that visualise the journey from making a request to receiving data. This is particularly helpful for parents who may be in a state of shock or cognitive impairment due to grief. Additionally, providers should offer "downloadable checklists" of the evidence required (e.g., birth certificates,

Question	Your response
	coronial letters) so parents can gather their documents offline and return to the process when they are ready. Another vital good practice is the "provision of glossaries and context" for technical decisions. If a platform refuses to share certain data because it is "end-to-end encrypted," it must explain in simple terms what that means and why it creates a technical barrier, rather than simply issuing a generic rejection. This fosters a sense of transparency and helps parents understand that the platform is not being intentionally obstructive. Furthermore, providers should ensure that their policies are "screen-reader compatible" and available in the languages most commonly used by their UK user base, ensuring that the "Right to Know" is not restricted by language or disability. Finally, good practice includes "user-centric feedback in policy design". Providers should be encouraged to consult with bereaved families and digital legacy experts—such as the "Bereaved Families for Online Safety" group—when drafting their disclosure policies. This ensures that the language used is genuinely helpful and sensitive to the needs of the people it is intended to serve. By involving those with "lived experience" of these barriers, service providers can move beyond "compliance" toward a genuine "service" model for bereaved families. **Table 3: Trauma-Informed Design Elements for Disclosure Policies**

<table>
<tr><th>Question</th><th>Your response</th></tr>
<tr><td></td><td>
<table>
<tr><th>Design Element</th><th>Traditional Approach</th><th>Trauma-Informed Approach</th><th>Postmortem Privacy Impact</th></tr>
<tr><td>Language</td><td>Legalistic; defensive; "The Company."</td><td>Empathetic; direct; "We are sorry for your loss."</td><td>Improves trust; reduces adversarial framing.</td></tr>
<tr><td>Navigation</td><td>Buried in T&Cs or Help pages.</td><td>Prominent, dedicated "Bereavement" portal.</td><td>Reduces "cognitive load" for grieving parents.</td></tr>
<tr><td>Visuals</td><td>Dense blocks of text.</td><td>Flowcharts; infographics; video guides.</td><td>Increases clarity for diverse demographics.</td></tr>
<tr><td>Explanation</td><td>"Request denied due to policy."</td><td>Reasoned decisions with specific privacy rationale.</td><td>Upholds dignity; provides "procedural justice".</td></tr>
<tr><td>Contact</td><td>No-reply email or generic form.</td><td>Dedicated case ID; named contact team.</td><td>Ensures sensitive, human-led communication.</td></tr>
</table>
</td></tr>
<tr><td>Question 7: Do you have any comments on our proposals in relation to how providers should provide a support function?</td><td>Confidential? – N

The proposal for a support function—which could be a helpline, a dedicated section of the service, or a live chat—is a critical component of the "Deceased Child User Duties". From a postmortem dignity perspective, the nature of this support is as important as its existence.</td></tr>
</table>

Question	Your response
	The support function should not be handled by the general customer service or content moderation teams, who may lack the training to handle the intense emotionality of bereavement requests. Instead, Category 1 services should be required to maintain a "dedicated bereavement support team" trained in trauma-informed communication and the specific legalities of digital remains. Furthermore, the support function must be "human-in-the-loop" by default. While automated FAQs are a useful starting point, parents should have a clear and immediate path to speak with a human agent. Automated systems often fail to account for the "nuance and sensitivity" required when discussing a deceased child's private life. A live chat or helpline provides a "safe space" for parents to ask questions about the disclosure process and receive guidance on the types of evidence needed, which can vary significantly depending on the family's specific circumstances. For smaller services (Category 2B or 2A), where a dedicated 24/7 helpline may not be "proportionate," the support function must still be "easily discoverable and responsive". A specific email address—e.g., "bereavementsupport@[service].com"—is far more effective than a generic "contact us" form. The Guidance should require these services to provide a "response timeframe" for support inquiries, ensuring that parents are not left waiting for days for a simple technical question to be answered. The goal is to provide a "navigational aid" that helps parents through the administrative maze without adding to their distress.

Question	Your response
Question 8: Do you have any comments in relation to the details about a support function which a provider of a relevant service must include in its terms of service?	Confidential? – N The details about the support function included in the terms of service (ToS) must be "specific and actionable". It is not enough for a provider to state that "support is available." The ToS should specify the "hours of operation" for the helpline, the "languages supported," and the "typical response times" for different types of inquiries. This level of detail provides a "service level agreement" for bereaved parents, allowing them to manage their expectations and plan their engagement with the platform during an incredibly chaotic time. Importantly, the ToS should clarify the "role of the support function". It should be framed as a tool to assist with the *procedure* of making a request and providing evidence, rather than a guarantee of the *outcome* of data disclosure. By being transparent about the "privacy and legal checks" that the support team must adhere to, the provider avoids giving parents a false sense of hope that they will receive "unfiltered access" to all of their child's data immediately. This protects both the provider from unrealistic demands and the deceased child's dignity from unintended over-disclosure. Finally, the ToS should include information on how the support function handles "conflicting claims". In cases where parents are separated or have differing views on whether to access the child's data, the ToS should outline the "mediation or legal verification" steps the service will take. Providing this information upfront ensures that the support function remains a neutral, helpful resource rather than becoming a site of further family conflict.

Question	Your response
Question 9: Are there other examples of good practice in relation to the provision of a support function or the details to be included in the terms of service we should also consider?	Confidential? – N A significant good practice for support functions is the implementation of "persistent case management". Having to retell a tragic story to a different agent every time they contact the service is a common source of "secondary trauma" for parents. Providers should assign a "named contact" or a "specialized case ID" so that a single team can follow the parent's request from start to finish. This creates a "relationship of trust" and ensures that the communication is as sensitive and efficient as possible. Another good practice is "proactive referral to external support". When a parent initiates a request, the support portal or agent should provide links to recognized bereavement charities, such as "Cruse Bereavement Support" or the "Molly Rose Foundation". This recognizes that the parent's "need to know" is often driven by a "need to heal," and the service provider has a "corporate social responsibility" to support that healing process. The support function should be a "gateway to care," not just a "gateway to data". Finally, providers should offer "technical assistance for data interpretation". If a platform discloses a large archive of data, it can be overwhelming for a parent to navigate. Good practice would involve providing a "guide to the archive" or a "tool for viewing" the data in a human-readable format, rather than just delivering raw JSON or CSV files. For parents seeking to preserve memories, the support function could offer help with "memorializing the account," which allows public content to remain as a tribute while closing private inter-

<table>
<tr><th>Question</th><th>Your response</th></tr>
<tr><td></td><td>actions. This respects both the "relational-living" interest in memory and the child's "post-mortal dignity".

Table 4: Levels of Support Function Complexity by Service Category

<table>
<tr><th>Feature</th><th>Category 1 (Largest U2U)</th><th>Category 2A (Search)</th><th>Category 2B (Smaller U2U)</th></tr>
<tr><td>Helpline</td><td>Mandatory 24/7 or high availability.</td><td>Recommended during business hours.</td><td>Highly recommended callback service.</td></tr>
<tr><td>Dedicated Team</td><td>Specialized "Bereavement & Legacy" team.</td><td>General "Legal & Safety" team with training.</td><td>Nominated "Safety Officer".</td></tr>
<tr><td>Support Portal</td><td>Interactive, searchable, multi-format.</td><td>Static, clear public statement.</td><td>Simple, clear help-centre section.</td></tr>
<tr><td>Case Management</td><td>Named contact/persistent case ID.</td><td>Email-based ticketing system.</td><td>Email-based ticketing system.</td></tr>
<tr><td>Referrals</td><td>Direct API/links to safety charities.</td><td>Links to support in search results.</td><td>Recommended links in ToS.</td></tr>
</table>
</td></tr>
<tr><td>Question 10: Do you have any comments on our proposal to align our guidance for how providers of relevant services should operate a complaints function with the approach</td><td>Confidential? – N

Aligning the complaints function with the Illegal Content and Protection of Children Codes is a sensible approach to ensure "procedural</td></tr>
</table>

Question	Your response
taken in the Illegal Content and Protection of Children Codes?	consistency". The requirement for the complaints process to be "easy to access, easy to use, and transparent" is a baseline for user rights under the Online Safety Act. However, the "appropriate action" resulting from a complaint under Section 75 must be "remedial" in a way that respects the "temporal sensitivity" of bereavement. If a parent complains that their request was ignored or that the redaction was overly aggressive, the platform must have a mechanism for a "senior manual review" rather than an automated appeal system. From a postmortem privacy perspective, the "transparency of the rationale" for decisions is the most critical element to align. Just as a user has the right to know *why* their content was removed under the Illegal Content code, a parent has the right to know *why* specific information about their child's use of the service was withheld. This "reasoned decision" should cite specific privacy grounds (e.g., third-party data protection) or legal barriers (e.g., lack of evidence of parental responsibility), allowing the parent to either provide additional evidence or appeal the decision to Ofcom. Furthermore, the "alignment" should include the requirement for "user-friendly reporting" on complaints. Providers should be required to include statistics on "deceased child user complaints" in their public transparency reports, including the number upheld and the average time to resolution. This ensures that the complaints function is not just a "dead end" for frustrated parents but a genuine mechanism for "regulatory accountability".

Question	Your response
Question 11: Do you agree with our proposal not to require providers of relevant services to operate a separate complaints function? Please explain why.	Confidential? – N The proposal not to require a *separate* complaints function is a pragmatic one, as it avoids "administrative fragmentation" for both the provider and the user. If a service already has a robust, accessible complaints infrastructure for illegal content or child safety, it is more efficient to "tag" or "categorise" bereavement-related complaints within that same system. However, this "non-separation" must not lead to a "loss of specialisation". Complaints regarding the "Deceased Child User Duties" involve a different set of legal and ethical considerations than general content moderation appeals. For this proposal to be effective, Ofcom must require that these complaints are "escalated to the specialised bereavement support team" mentioned in Question 7. A general content moderator may not understand the "postmortem dignity" lens or the specific requirements of Section 75. Therefore, while the *entry point* for the complaint can be the same, the *adjudication* must be performed by staff with the appropriate training and sensitivity. Additionally, the "non-separate" system must ensure that these complaints are "prioritised". Bereavement-related issues should not be buried under a high volume of lower-priority complaints (e.g., about minor account suspensions). The Guidance should recommend that providers implement a "sensitive case" flag that ensures these complaints are handled with the urgency and "dignity" that the Act requires. This "integrated but specialised" approach provides the best balance of efficiency and empathy.

Question	Your response
Question 12: Do you have any comments on our proposal in relation to easily accessible policies and processes that govern the handling and resolution of such complaints?	Confidential? – N Easily accessible policies for handling and resolving complaints must provide a "clear procedural map". Parents should know exactly what to expect after they file a complaint: 1) Who will review it? 2) What is the timeframe for a response? 3) What are the possible outcomes? 4) How can they appeal further?. This transparency reduces the "power imbalance" between the individual parent and the massive tech platform. Accessibility also means providing "templates and guidance for complaint-drafting". Many parents may be overwhelmed and unsure how to articulate their legal concerns under the Act. Providers should offer a "simple form" with drop-down menus that help parents specify their issue—e.g., "Delay in response," "Incomplete disclosure," or "Verification difficulties". This "structured accessibility" ensures that the complaint contains all the necessary information for a rapid resolution, benefiting both the parent and the service provider. From the perspective of "procedural justice," the policy should also specify the "independence of the reviewer". Good practice would dictate that a complaint about a disclosure decision should be reviewed by someone who was not involved in the original decision. This ensures "impartiality" and helps parents feel that their concerns are being taken seriously. Finally, the policy must be available in "plain English" and "accessible formats" (e.g., audio, large print), ensuring that all bereaved parents have equal access to "redress".

Question	Your response
Question 13: Are there any further examples of good practice in relation to the operation of a complaints function or the provision of relevant provisions in the terms of service we should consider?	Confidential? – N A critical good practice for the complaints function is the "provision of a second-tier review" or an "independent ombudsman". If a parent is dissatisfied with the platform's internal resolution, the service should provide clear information on how to escalate the matter to an independent body or a specific regulatory contact at Ofcom. This "external accountability" is essential for building public trust in the new regime. Another good practice is "qualitative resolution". Instead of just issuing a "Yes/No" decision, providers should offer "clarification calls" or "written summaries" that explain the complex privacy considerations that led to a specific decision. For example, if data was withheld to protect a third party's "Article 8 rights," explaining this context can help the parent understand that the decision is rooted in "rights balancing" rather than corporate obstruction. Finally, providers should use "anonymized complaint data for continuous improvement". Good practice would involve a periodic review of all bereavement-related complaints to identify "systemic friction points" in the disclosure process. These findings should inform the "safety-by-design" updates to the service, ensuring that the "Deceased Child User Duties" become more effective and less traumatic over time. This "iterative learning" model demonstrates a genuine commitment to the "dignity and respect" of bereaved families. **Table 5: Procedural Standards for Complaint Handling**

<table>
<tr><th>Question</th><th>Your response</th></tr>
<tr><td></td><td>
<table>
<tr><th>Stand-ard</th><th>Requirement</th><th>Postmortem Privacy lens</th></tr>
<tr><td>Visibil-ity</td><td>Prominent links in ToS and Support portals.</td><td>Reduces "navi-gation trauma".</td></tr>
<tr><td>Impar-tiality</td><td>Review by a differ-ent team than the original decision-makers.</td><td>Ensures "proce-dural justice" for families.</td></tr>
<tr><td>Specific-ity</td><td>Reasoned decisions citing specific le-gal/privacy grounds.</td><td>Upholds the "dignity" of the child's data.</td></tr>
<tr><td>Timeli-ness</td><td>Resolution within 15–20 working days.</td><td>Recognises the urgency of grief.</td></tr>
<tr><td>Re-course</td><td>Clear path to inde-pendent review or Ofcom escalation.</td><td>Limits platform "unilateralism".</td></tr>
</table>
</td></tr>
<tr><td>Question 14: Do you have any com-ments on the; impact assessment; rights assessments; equality impact assessment; and Welsh language im-pact assessment. Please provide any information or evidence in support of your views.</td><td>Confidential? – N

The Impact Assessment and Rights Assess-ment are perhaps the most vital documents for ensuring that the "Deceased Child User Duties" do not inadvertently infringe on the very rights they seek to protect. From a post-mortem privacy perspective, the current as-sessment appears to "underestimate the in-terference with Article 8 ECHR". Ofcom's claim that its approach is "unlikely" to interfere with privacy rights is problematic. Any disclosure of a deceased child's private data is an interfer-ence with the child's postmortal privacy and the correspondence rights of third parties. While this interference may be "justified and proportionate" under Section 75, it must be</td></tr>
</table>

Question	Your response
	explicitly acknowledged as such to ensure a rigorous "balancing exercise". The Rights Assessment should more deeply integrate the "Best Interests of the Child" principle. My research emphasises that adults and children have an interest in "digital self-determination" that persists after death. A robust assessment must consider the "future-decedent interest" of living children—if they believe their data will be fully disclosed upon death, they may self-censor or lose trust in digital spaces. The Impact Assessment should also account for the "risk of harm to third parties," particularly the child's peers, whose intimate correspondences may be revealed to an adult (the parent) without their consent. This necessitates the "mandatory redaction" measures discussed in Question 2b. Furthermore, the "Equality Impact Assessment" should address the "digital divide in bereavement". Vulnerable parents, those without standard government IDs, or those for whom English is a second language, may face "discriminatory barriers" to exercising their "Right to Know". The Guidance must require providers to accommodate "alternative evidence" and provide support in "multiple languages" to ensure equitable access to closure. Finally, the Impact Assessment should recognise the "positive privacy impact" of transparency—if users (both children and parents) understand the conditions of disclosure, they can make better-informed choices about their "informational body and footprint" during their lifetime. **Synthesised Conclusions and Policy Recommendations**

Question	Your response
	The successful implementation of Section 75 requires a nuanced understanding of "post-mortem dignity". For the Guidance to be effective, it must move beyond general safety principles and embrace the specific complexities of digital remains and postmortem privacy. The central challenge for Ofcom and service providers is to facilitate the parental "need to know" while respecting the child's "right to be left dead". This requires a move away from "binary disclosure" (all or nothing) toward a "granular, contextual disclosure" model. By prioritising "human-in-the-loop" review, manual redaction, and specialised bereavement support, platforms can fulfil their duties under the Act while upholding the fundamental dignity of the deceased child and the privacy of their living peers. The following recommendations summarise the core expert-level feedback for the final Guidance: 1. **Adopt a Restrictive Interpretation of Disclosure**: Providers should disclose only what is "necessary and relevant" to the parent's inquiry, using redaction to protect the child's most intimate secrets and third-party data. 2. **Codify Hard Timeframes**: "Timeliness" should be defined as 20–30 days for a substantive response, with mandatory progress updates to alleviate parental distress. 3. **Mandate Specialised Training**: Support and complaints functions must be staffed by teams trained in "digital legacy" and "trauma-informed communication".

Question	Your response
	4. **Promote Pre-Mortem Autonomy**: Encourage the use of "Legacy Contact"-like tools (adapted to children's needs and development) during the child's life to ensure their own wishes are the primary guide for postmortem data handling. 5. **Rigorous Rights Balancing**: The Guidance must provide a clear framework for weighing the "relational-living" interest of parents against the "informational body" rights of the deceased and the data [protection and Article 8 rights of third parties. By implementing these measures, Ofcom can ensure that the Online Safety Act becomes a model for the world—a regime that provides families with the answers they need for closure while treating the "informational body" of the child with the same reverence and respect as their physical remains. The digital age requires a "new social contract for mortality," and this Guidance is a vital first step in drafting it.

Please complete this form in full and return to DCUguidance@ofcom.org.uk.