Technology Notices to deal with terrorism content and/or CSEA content

Annexes 11-14: Technical Information relating to minimum standards of accuracy proposals

Consultation

Published: 16 December 2024
Closing date for responses: 10 March 2025

Contents

Annexes

A11. Example questions for the audit-based assessment

A11.1 To help applicants understand what evidence to provide in support of each objective included in the audit-based assessment, and to ensure a consistent approach to scoring by Ofcom or the nominated third party, a list of questions would be produced for accreditation. These questions would correspond to each of the objectives and provide greater detail on the evidence required to score full or partial marks against the objective. There would likely be multiple questions for each objective.

A11.2 We have set out some examples of the types of questions we would expect to ask and the format in which they could be presented to applicants. These are for illustrative purposes only and are not an indication of whether the same or similar phrasing or style of question would be included as part of the accreditation scheme.

Technical Performance	
Objective	Performance Metrics: The technology has been comprehensively evaluated against appropriate performance metrics, and reported performance metrics along with their corresponding results are provided.
Example Question	**Evidence Levels / Scores**
What is the overall technical performance of the technology? Provide documented evidence of how accuracy is measured, and the results obtained.	**Level 0 (0 points):** No evidence provided or anecdotal evidence without any quantitative evaluation results. *Example of received documentation:* None, or statements lacking quantitative data. **Level 1 (1 point):** Internal test results on limited or insufficiently diverse datasets. Basic metrics (e.g., accuracy only) without detailed breakdown. *Example of received documentation:* Internal testing reports, basic precision and recall metrics on limited dataset descriptions. **Level 2 (5 points):** Comprehensive results from large-scale, diverse, and representative datasets, including breakdowns by harmful and non-harmful content (content type, language, and scenario). Detailed analysis with confusion matrices, receiver operating characteristic (ROC) curves, and accuracy across all relevant metrics. *Example of received documentation:* Comprehensive evaluation reports, confusion matrices, ROC curves, detailed dataset descriptions, extensive breakdowns of accuracy by various factors. Benchmarking reports, dataset descriptions, detailed metric results including precision-recall curves, confusion matrices, F1 scores, analysis of false positive rate (FPR) and false negative rate (FNR) across diverse datasets and content types.

Fairness	
Objective	Bias Identification: Comprehensive policies, procedures, metrics and analyses have been implemented to identify potential biases in the technology, throughout planning and development.
Example Question	**Evidence Levels / Scores**
What are the potential biases that may arise in the way the technology has been designed and developed? Are such bias risks appropriately identified throughout the lifecycle of the technology? Provide documented evidence of risk assessment processes, including any frameworks or tools used to evaluate bias risks.	**Level 0 (0 points):** No identification of potential biases is made during the design and development stages or documentation of bias risk assessments or mitigation strategies. *Example of received documentation:* None. **Level 1 (1 point)**: Basic identification of potential biases is made, but it may be incomplete or lacking in depth. Some documentation of bias risk assessments may be available, does not cover the entire lifecycle. *Example of received documentation:* Basic documentation of potential biases identified, limited bias risk assessment reports, and minimal evidence of lifecycle-wide mitigation strategies. **Level 2 (5 points):** Advanced and continuous identification of potential biases is integrated throughout the entire lifecycle of the technology. Documentation is extensive, showing clear evidence of thorough bias risk assessments, continuous monitoring, and proactive mitigation strategies at every stage of development. *Example of received documentation:* Extensive documentation of potential biases identified, rigorous bias risk assessment reports, continuous records of bias monitoring, and proactive mitigation strategies.

Robustness	
Objective	Detection and Mitigation of Threats: Sufficient safeguards and processes are in place to detect and mitigate both intentional and unintentional threats, which may include input manipulation and contextual misunderstandings. The technology can effectively respond to a wide range of adversarial attacks and circumventions of intended use while maintaining its integrity and accuracy.
Example Question	**Evidence Levels / Scores**
How does the technology perform when subjected to input perturbation attacks, such as adding noise, altering colours, or modifying words? Provide documented evidence from perturbation testing, including results that showcase the technology's resilience to deliberate alterations in input data. Evidence of any tests done on the technology using data that has undergone transformations (e.g., pixelation, rotation, resizing), including (if applicable) how results from altered data replicate or differ from results on unaltered data.	**Level 0 (0 points):** No documentation of performance under input perturbation attacks, or no evidence of resilience. *Example of received documentation:* None. **Level 1 (1 point):** Basic perturbation tests with limited documentation and partial evidence of resilience. *Example of received documentation:* Documentation of basic perturbation tests, records of limited resilience outcomes, and partial analysis of results. **Level 2 (5 points):** Extensive perturbation testing with thorough documentation, continuous monitoring, and evidence of the technology's robust defence against input perturbations. *Example of received documentation:* Comprehensive documentation of extensive perturbation tests, detailed records of resilience across multiple scenarios, continuous monitoring reports, and evidence of sustained robustness. Detailed documentation of tests on various data transformations, comprehensive records of results, and evidence of consistency or significant findings in comparison with unaltered data.

Maintainability	
Objective	Comprehensive Documentation and Policies: Sufficient development documentation, risk management, and data retention policies have been implemented and executed. This ensures that the performance of the technology is well-documented and managed throughout its lifecycle. Clear accountability for the documentation and management of the technology exists, and the accountable person(s) are identified.
Example Question	**Evidence Levels / Scores**
Explain and provide evidence for the organisation's data retention policies as they relate to this technology.	**Level 0 (0 points):** Data retention policies and procedures do not exist or are not enforced. *Example of received documentation:* None. **Level 1 (1 point)**: Data retention policies exist but may be inconsistently enforced, insufficiently cover relevant data, or fail to preserve data for a reasonable period of time. *Example of received documentation:* Basic data retention policies, partial enforcement records, or limited scope of coverage. **Level 2 (5 points):** Data retention policies are comprehensive, enforced consistently across the organisation, and include regular audits. Policies cover all relevant data types and ensure data is preserved for appropriate durations. Evidence of policy updates is provided. *Example of received documentation:* Detailed data retention policies, audit reports, records of consistent enforcement, and regular policy review logs.

A12. Provisional Metrics for independent performance testing

A12.1 Below we outline the list of metrics (in alphabetical order) for which we propose to calculate benchmarked thresholds as part of the independent performance testing if this were to form part of the minimum standards of accuracy. These would be used to evaluate the performance of technologies submitted for accreditation in all testing categories.

A12.2 **Accuracy**, which measures how often a model correctly predicts the outcome by dividing the number of correct predictions (true positives and true negatives) by the total number of predictions, to determine the proportion of all classifications that were correct.

A12.3 **F1 Score**, which is the harmonic mean of precision and recall and provides a single measure of a model's accuracy that balances both false positives and false negatives. It is calculated as the product of precision and recall divided by the sum of precision and recall, multiplied by two.

A12.4 **False Negative Rate**, which refers to the proportion of positive cases incorrectly predicted by a classification system as negative cases. In other words, the system predicts that the example is negative, and it is actually positive.

A12.5 **False Positive Rate,** which refers to the proportion of negative cases incorrectly predicted by a classification system as positive cases. In other words, the system predicts that the example is positive, and it is actually negative.

A12.6 **Latency,** which measures the time it takes for the technology to process one data unit and produce a classification result, calculated by the time taken to process a single unit of data from input to output.

A12.7 **Matthews Correlation Coefficient (MCC)**, which is the harmonic mean of precision and recall for both positive and negative classes and provides a single measure of a model's accuracy that balances true positives, true negatives, false positives, and false negatives.

A12.8 **Precision**, which measures the percentage of how many items that were predicted as 'positive' are true positives.

A12.9 **Throughput**, which measures the rate at which a system processes data to produce outputs over a specific period, calculated by the number of data units processed per unit of time.

A12.10 **True Negative Rate**, which refers to the proportion of negative cases correctly predicted by a classification system. In other words, the system predicts that the example is negative, and it is actually negative.

A12.11 **True Positive Rate (Recall),** which refers to the proportion of positive cases correctly predicted by a classification system. In other words, the system predicts that the example is positive, and it is actually positive.

A13. Data considerations for setting the minimum standards of accuracy

A13.1 If independent performance testing were to form part of the minimum standards of accuracy, Ofcom or a third party appointed by Ofcom would need to obtain and maintain datasets suitable for testing different types of technology.

A13.2 In this annex we set out our understanding of the data needed to conduct this testing, and our proposed approach (at a high level) to datasets.

A13.3 We have included this detail here to support respondents in considering our core proposals. This is important given the central role of data testing in one of our proposed approaches. This annex covers the following:

a) What data would need to be obtained for effective performance testing, and why.

b) How data could be sourced.

c) Properties of the data that may be relevant or desirable when sourcing data.

d) Measures to reduce the risk that the testing data might have been previously used to develop and test the technologies.

e) How data can be quality-assured and updated over time.

Illegal and benign data

A13.4 The minimum standards of accuracy against which technology would be accredited relate to the detection of terrorism and/or CSEA content. It therefore follows that if independent performance testing forms part of the minimum standards of accuracy, the data which technologies are tested against must include some terrorism and/or CSEA data, which we will refer to, collectively, as illegal data. It would also need to include other data, which we will refer to as benign data.

A13.5 The illegal data is necessary to confirm and evaluate the technology's capability to accurately detect such content, while the benign data acts as a control group, to evaluate the technology's capability to distinguish between the two kinds.

A13.6 We would expect the technologies that are being tested to be mainly operating in environments where there is predominantly benign data. This means the dataset that is used in any independent performance testing would ideally reflect that likely reality, meaning that Ofcom would have to consider whether the datasets would need to be imbalanced. We recognise that there is a low prevalence of terrorism and/or CSEA content on most services. However, when collating such datasets, Ofcom may still aim to include higher proportions of harmful data than would reasonably be expected for common use cases of relevant technologies, to reflect the need to test the primary capabilities of safety technologies in correctly detecting or classifying harmful data.

A13.7 The illegal data in the dataset would be labelled according to the kinds of harm it relates to. The benign data should be representative of the presumed variation and respective

likelihood of a technology processing such data when deployed by a regulated online service. It should also, ideally, include a higher proportion of some specific kinds of benign data, such as if the data could be considered a near-neighbour of the illegal data.[1]

Data collection

A13.8 Ofcom would need to conduct further work to understand how relevant datasets could be sourced. We may consider collecting such datasets from a variety of sources, including publicly available datasets. We would do this by commissioning the collection of bespoke datasets from contractors with suitable expertise, and by using our information gathering powers. It will be more difficult to acquire some CSEA content from comparable sources, as much of it is illegal to hold unless specific legal defences apply, so the possession of such data may be unlawful for these kinds of data sources. In such circumstances Ofcom may seek to acquire datasets from law enforcement agencies through bespoke agreements.

A13.9 When collecting data, Ofcom need to consider the data types, categories, and themes in those already collected and those considered. Unless otherwise required, we do not propose to identify any of the collected datasets.

Data types

A13.10 The concept of data types refers to distinct kinds of data that are grouped based on their format and how it is stored on an electronic medium. In the context of accrediting technologies, these types may include image, audio, video, text, URL, and hash.[2]

Data categories

A13.11 Data categories are classifications within a data type that distinguish data based on the nature and format of its content. They provide a mechanism to understand and categorise data in relation to its specific form or presentation. Data categories reoccur across datasets and types, further specifying the format, structure, or content of the data. This can include synthetic data created from other data.

A13.12 We have provided examples of such data categories for different data types in Table A1, below. These are for illustrative purposes only and the existence or absence of any data category in these examples is not an indication as to whether Ofcom considers them relevant for its approach to accreditation.

[1] A near-neighbour of relevant content is content that shares some crucial, indicative characteristics with relevant content but is not relevant content itself. For example, pornographic content may be considered a near-neighbour of CSEA content, and religious content for some terrorism content.

[2] Metadata, which may be considered a data type of its own or a mix of others, is expected to be a lower priority in the first instance. Ofcom may conduct further work to explore the variety and variations of metadata. The data types URL and hash are content agnostic, and are not applicable to the subsequent sections on data categories, themes, and transformations.

Table A1: Data category examples

Data type	1	2	3	4	5	6	7
Image	Cartoon / anime	Drawing	Diagram	Logo	Map	Meme	Photograph
Video	Amateur pornography	Documentary	Fitness / workout	Livestream	Movie trailer	Video blog / vlog	Virtual reality
Audio	Ambient sound	Audiobook	Live music	Podcast	Radio news	Sound effect	Speech
Text	Computer code	Cooking recipe	Interview transcript	Movie reviews	News article	Novel / book	Poetry

Data themes

A13.13 Data themes are conceptual constructs based on commonalities of the represented, depicted, or otherwise contained content within data. They provide a way to categorise and understand data in relation to its content. Data themes are not exclusive to data types or categories and may reoccur across them. Most content is associated with multiple themes.

A13.14 Table A2 provides examples of data themes for different data categories. These are for illustrative purposes only and the existence or absence of any data theme in these examples is not an indication of whether Ofcom considers them relevant for its approach to accreditation.

Table A2: Data theme examples

Animals	Architecture	Cities	Dance	Education
Fashion	Festivals	Health	Literature	Nature
People	Religion	Social gathering	Sports	Technology

Data transformations

A13.15 Data transformations play a crucial role in assessing the performance of technologies under simulated real-world conditions. Under real-world conditions, data commonly undergoes intentional and unintentional transformations, altering how content may be perceived by users or modifying the data's underlying technical structure. To assess the accuracy of technologies, some data items in the testing datasets will need to undergo one or more such transformations.

A13.16 Table A3 provides illustrative examples of such data transformations for visual (image and video), auditory and text data types. These are for illustrative purposes only and the

existence or absence of any data transformation in these examples is not an indication as to whether Ofcom considers them relevant for its approach to accreditation.

Table A3: Data transformation examples

Data type	1	2	3	4	5	6	7
Visual (image & video)	Cartoonify	Crop	File type change	Overlay	Resize	Rotate	Shape change
Audio	Ambient / background sound	Echo effect	File type change	Pitch change	Trim	Sampling frequency reduction	Sampling rate change
Text	Capitalise	Homoglyph	Mirror	Paraphrase	Synonym	Substitute character	Upside-down

Data secrecy

A13.17 The independent performance testing of technologies needs to be as objective and free from bias as possible, to ensure validity and reliability of the results. This means that ideally, the data on which technologies are tested should be distinct from any data used during the development of technologies. This is particularly pertinent because the terrorism/CSEA content detection technologies being tested are likely to include those involving machine learning or other data-driven algorithms. Where the development of technologies involves machine learning, the data is typically used as a direct input, while other technologies, such as rule-based technologies, typically require knowledge of relevant data by the developers.

A13.18 This poses a challenge for Ofcom, as we cannot ensure that the data we, or a third party instructed by us, would use for technology accreditation has not been used to develop any such technologies.[3] To mitigate this risk, we are proposing to sub-sample the datasets from several relevant datasets. The idea is to randomly select a subset of data from a large data source, and to withhold knowledge of which data source the subset was sampled from. As the subset is randomly selected, and if the data is sampled from several sufficiently large data sources, the likelihood that a technology has encountered this specific subset of the data during its development is significantly reduced. We believe that this is a suitable proxy

[3] For some kinds of data, such as indecent images of children, it would be unlawful in most cases for the developers of safety technologies to hold such data themselves, but they could have entered into collaboration agreements with entities who have a valid legal defence.

for a withheld dataset,[4] though Ofcom may need to conduct further work to understand residual limitations.[5]

A13.19 To address the risk that a sub-sampled dataset will not be sufficiently free of bias, Ofcom is proposing the use of stratified sub-sampling. This approach divides the large data source into different strata before sub-sampling from each stratum in equal proportions. Data and dataset characteristics to define strata can be qualitative (for example, subsampling one stratum from a dataset where approximately 90% of images are pictures of religious content) and quantitative (for example, subsampling one stratum as only greyscale pictures from a dataset of CSEA content). All relevant kinds of data should be represented in the sub-sampled dataset. This also enables Ofcom to influence the quantity of data sampled from each stratum, such as when it is desired to increase the representation of certain near-neighbour data.

Data quality assurance and updates

A13.20 Data quality assurance is a critical step in data management, especially when data is sourced from third parties. We would expect to take reasonable steps to validate the data's quality to assure its accuracy, reliability, and integrity.

A13.21 When dealing with large datasets, it may not be feasible to inspect every single data item. In such cases, we would expect to inspect a random sample instead. If the sample passes the quality assurance process, we can reasonably infer that the rest of the dataset is also of sufficient quality. The choice of a suitable sampling method will depend on dataset properties, such as the kind of data, its labels, and whether it is organised in an existing data structure. We expect that one of the following sampling methods will usually be a suitable method: simple random sample, stratified random sample, cluster random sample, and systemic random sample.[6]

A13.22 Various data validation checks can be used to assess the data quality. The selection of checks will depend on the kind of data and its intended use. Most datasets will be subject to multiple validation checks. The following are examples of validation checks Ofcom may consider, depending on the kind of data and its intended use:

a) **File type check**: This ensures that the data is of the expected type, such as text string, image (e.g., .jpeg) or video (e.g., .mp4).

b) **Format check**: This validates that the structure inside a file is as expected, such as ensuring that where multiple individuals participate in a text-based conversation, each participant has a unique label and each message exchanged is labelled correctly.

[4] A 'withheld' dataset refers to a set of data that is intentionally kept separate and not used during technology development, but reserved for later use to evaluate the technology's performance and ensure it generalises well to new, unseen data.

[5] For example, where Ofcom might be unable to acquire several datasets of content from which it could subsample, such as for indecent images of children, it may affect the reliability of testing technologies to detect unknown harmful content which may have been trained on large parts of the same data. One avenue to mitigate such impacts could be through additional testing prior to issuing a Technology Notice on data collected after a technology was submitted for accreditation.

[6] A simple random sample gives every data item an equal chance of selection; a stratified random sample divides the dataset into subgroups or strata and samples from each; a cluster random sample selects entire groups or clusters of data randomly; and a systematic random sample picks every n^{th} data item after a random start.

c) **Uniqueness check**: This ensures that each data entry is unique and there are no duplicates.

d) **Correctness check**: This verifies that the data is correct, often by validating expectations on the content of the data or comparing it to a known standard or benchmark.

e) **Consistency check**: This ensures that the data is consistent across the dataset, meaning that it follows the same rules or conventions.

f) **Range check**: This validates that the data falls within a specified range, such as file size or image dimensions.

g) **Distribution check**: This ensures that the data matches expected patterns or statistical properties, such as where a dataset containing terrorist publications should contain certain minimum quantities of content related to different proscribed organisations.

A13.23 The outcome of the data quality assurance may affect the number of samples we would take from a dataset. For example, there may be scenarios where a desirable characteristic in a dataset is represented in smaller quantity than anticipated or where data with the desirable characteristic is also prevalent in another dataset which has already been sampled from.

A13.24 Over time, the datasets we use to test technologies against would need to be updated. First, as technologies evolve, new kinds of data will need to be processed by relevant safety technologies and thus will often need to be represented in relevant datasets used for testing those technologies. Second, as society evolves, the makeup of data typically prevalent on relevant regulated services will not only fluctuate within certain boundaries but also exhibit larger long-term shifts beyond those – a phenomenon also known as a domain shift.

A13.25 Given the amount of time and resource needed for data collection and quality assurance, Ofcom will need to undertake these processes one data type at a time. It may also be necessary to have mixed-type datasets that include multiple data types. Typically, data items from the different type of data in these mixed datasets should be paired,[7] such as memes, in which images and text are positioned together. Where a technology is capable of processing unrelated data of multiple types, it may be evaluated based on its performance on the corresponding single-type datasets. While we initially do not consider the creation of such mixed-type datasets would be a priority, we also do not preclude that we may create them in the future.

[7] In this context, 'paired' refers to the relationship between data items from different types of data within a mixed dataset, where each data item from each type of data is directly associated with another data item from another type of data within that mixed dataset. For example, a mixed dataset related to terrorism fundraising campaigns might have videos alongside text descriptions or calls to action, and each video in the mixed dataset should have at least one text associated, and vice versa. This is notwithstanding the fact that there may be additional datasets related to terrorism fundraising containing only videos or only text.

A14. Accreditation Application Template

A14.1 As explained in Section 2, accreditation is not the focus of this consultation document. However, in this annex, we have set out an illustrative example of the information that we are likely to request from technology developers seeking accreditation before their technology is put forward for evaluation against the minimum standards of accuracy. While we are not explicitly seeking stakeholders' views on this, they are welcome to provide comments on this should they wish.

A14.2 Applicants would be asked to provide comprehensive details about their technology using the draft form set out below (or a customised variant), which would undergo an initial completeness check before further evaluation. The purpose of this information would be to provide vital context to support the accreditation process and allow Ofcom, or a third party nominated by Ofcom, to assess the technology more thoroughly during later stages. It should help Ofcom understand the suitability of the technology for accreditation and determine which other technologies it may be benchmarked against during independent performance testing, if conducted. It would not be used to determine whether the technology meets the minimum standards of accuracy.

A14.3 Applicants are required to have the information in this submission signed off by an individual with sufficient seniority within their organisation. This step will ensure that the submission has undergone appropriate internal governance before being submitted for consideration, even if it does not guarantee completeness or accuracy.

A14.4 To facilitate a structured review, technology developers are requested to provide details across the following categories:

Information Category	Details
Description of the Technology	**Name:** [Technology Name] **Purpose:** Provide a brief overview of the technology, including its intended purpose and key functionalities. Explain if it's an AI-powered solution, a hybrid of AI and non-AI components, or a non-AI technology. Specify whether the technology is a machine learning model, rule-based model, software application, or another type of technology. Also, mention if it includes multiple consecutive or layered processes (e.g. pre-processing, core models, post-processing). Include details on the problem it aims to solve and its typical application scenarios. **Trust & Safety Application:** Provide a brief overview of whether the technology applies to user-to-user services, search services, or both. Additionally, indicate whether it is intended for use on messaging, search, livestreaming, or other service functionalities. **Human Review:** Specify if the technology is designed to require human review of all detected content, partial human review, or if it facilitates automatic takedown decisions without human intervention.
Harm Type	**Categories**: [Terrorism or CSEA] **Details**: Describe which particular terrorism and/or CSEA offenses the technology is capable of detecting (e.g. terror propaganda and terror flags). Additionally, clarify how the technology interacts with these harms – whether it is designed to detect harmful content (by identifying it when it appears), prevent it (by blocking its distribution or access), or mitigate its effects (by flagging, reporting, or removing it).

Entity / Organisation	**Entity Name**: [Organisation/Individual Name] **Contact Information**: Provide contact details for the organisation or individual responsible for developing and maintaining the technology. **Ownership**: Explain the ownership structure, including any partnerships or collaborations. **Organisation Type**: Provide details about the organisation type (for-profit, non-profit, academic, public sector, etc.) **Organisational Size**: Provide details about the size of organisation, including number of employees.
Modality	**Supported Modalities**: Specify the types of data the technology can process (e.g. image, video, metadata, text, audio, multimodal). **Use Cases**: Describe how the technology operates across different modalities, if applicable.
Data Requirements	**Input Data Format**: Specify the types of data format required for the technology to function (e.g., .png, .pdf, .gif, .doc). **Data Volume**: Indicate the minimum, optimal, and maximum amounts of data needed for effective operation. **Data Pre-processing**: Describe any data quality standards or pre-processing needed before data can be used.
Outputs	Provide details on the output generated by the technology (e.g. confidence scores, probability, text classifications, image annotations, video analysis reports). Specify the format (e.g. JSON, XML, CSV) and any standard or custom schemas used.
Language (if applicable)	**Supported Languages**: List the languages the technology can process, including input and output languages, if applicable. **Language Support Details**: Explain how language processing is handled (e.g., through machine translation, specific language models) and any limitations in language capabilities.
Geography	**Development Location**: Indicate where the technology was developed (e.g. country, region). **Deployment Regions**: Provide details of the regions or countries where the technology has been deployed, and any geographical limitations or optimisations.
Previous Deployment	Detail previous instances where the technology has been deployed, including (if available) the name of organisations, dates, and specific use cases. If applicable, provide case studies or examples of how the technology was used, including the outcomes and any challenges faced.
Previous Accreditation	**Previous Accreditation:** Provide information regarding any previous accreditations of this technology by Ofcom against the minimum standards of accuracy for use in Technology Notices. If technology has been previously accredited for use in Technology Notices, provide information on the following: **Versioning**: Indicate the version of technology that was previously accredited, and any version history since that point. **Change Log**: Provide a summary of significant changes in each version (e.g. bug fixes, algorithm improvements) since the point of previous accreditation.
Resourcing	Provide details on the computational resources needed to deploy the technology, including CPU/GPU specifications, memory, and storage requirements. Additionally, provide details on the technology's ability to scale, including how it handles increased input volumes, concurrent processing, and whether it supports distributed computing.
Dependencies	**Required Technologies**: List any software, hardware, or third-party services that the technology relies on for operation (e.g. specific libraries, cloud services, operating systems, existing models). **Interoperability**: Explain how these dependencies are integrated and any potential risks or issues related to them. **Adaptation**: If applicable, provide information about any existing models or algorithms (open-source or otherwise) that the technology has been directly adapted from.

Compatibility	**Client/Surface Compatibility**: Provide details on the extent to which the technology can be used across different platforms (e.g. desktop, mobile, web). **Deployment Environment:** Specify the target deployment environment (e.g. cloud, on-premises, edge). **Cross-Platform Integration**: Explain any specific requirements or limitations for different clients or surfaces (e.g. browser compatibility, mobile OS versions).
Privacy and Legal Considerations	**Data Protection:** Explain how the technology handles user data, including collection, storage, processing, and any measures taken to anonymise or pseudonymise data. Additionally, provide information on whether the technology developer has ever been found in breach of UK data protection requirements, and if so, what actions have been taken to address these issues. **Information Security and Access Control**: Detail the protocols in place to protect data from unauthorised access and explain how access to the technology is managed and monitored. **Previous Legal Convictions:** Outline whether the organisation has any legal convictions, e.g. under section 7 of the Bribery Act 2010, along with details of the steps taken to resolve the matters leading to any conviction.
Known Limitations and Known Caveats	**Acceptable Use**: Provide any documentation produced regarding scenarios where the technology should not be deployed, including the acceptable use policies applicable to the technology. **Operational Considerations**: Explain any operational considerations, such as: scenarios where the technology may not function as intended, performance issues under certain operational conditions, or challenges with specific data types and/or sizes.
Licensing and Pricing	**License Type:** Specify the type of license under which the technology is distributed (e.g., open-source, proprietary). **Distribution Methods:** Describe whether the model will be available as a SaaS solution, API integration, standalone software, or on-premises installation. Also, describe any necessary infrastructure for deployment (e.g. specific cloud platforms, edge devices, or data centres), performance issues under certain conditions, hardware dependencies, or challenges with specific data types how does the distribution method impact the scalability and latency of the model. **Pricing Model:** Provide details on the pricing structure (e.g. subscription-based, one-time purchase, freemium).
Sign-Off	**Name, Position, Signature, Date of Signature, and Email Contact**