Department for Education

Technology Group
Enabling you to deliver
Stabilise.
Optimise.
Transform.

2nd Condition Data Collection Programme
IT Solution
*** INVITATION TO TENDER ***
VOLUME 2 – STATEMENT OF REQUIREMENTS

Contents

REQUIREMENTS

1.1 Basic Terminology

Throughout this Statement of Requirements the following terms are commonly used. All other terms not specifically defined in this Statement of Requirements shall be construed as defined in the Agreement:

“CDC2 Process” – the documented process for the CDC2 Programme covering Surveyor mobilisation, resourcing, collection of data, checking of data, auditing of data and release of data to schools. The CDC2 Process is split into 6 stages (see Appendix D and Appendix E).

“Data status” – for any establishment’s survey data, the ‘status’ of that data is dictated by which stage of the CDC2 Process it is currently ‘in’. E.g. “SO Approved” status is reached at completion of Stage 4 “SO Quality Assurance”. The different data statuses are illustrated in Appendix D.

“DfE” – the Authority as defined in the Agreement.

“Integrated Audit Functionality” – the functionality available within the web app to enable structured audit of data.

“Mobile App” – an app or ‘technology solution’ hosted on a mobile device which allows SOs to collect validated data on site.

“SO” – one of the 3 Surveying Organisations appointed by the DfE to undertake the surveying services.

“Survey” – the data created for a specific establishment encompassing all data collected by Surveyors whilst on site, photos, site plans, and any other data such as DfE unique reference identifier relevant to that site.

“Surveyor(s)” – the Surveyor(s) engaged by one of the SOs to conduct the surveying services.

“Survey Section” – a sub set of data points / questions within a Survey. E.g. ‘Site level questions’, ‘Block level questions’.

“Tranche” – surveying will take place over the course of the programme over 10 surveying tranches. This enables the DfE and SOs to effectively manage the pace of programme delivery. The majority of the tranches will contain around 2700 establishments, with a final mop up tranche and an FE establishment tranche scheduled near the end of the 5 year CDC2 Programme.

“Web-App” – a hosted web app portal, providing data access, reporting and editing capability.

Please see the Glossary for explanation of other terms.

1.2 High level business user requirements

The Supplier Solution must support the following high level data ‘flow’. A diagrammatic overview can be found in *Appendix D: Data Status and CDC2 Deliver Process Stages*.

Migration / Import

- Import of all relevant DfE provided reference and legacy data to the Supplier Solution, noting that this may require ETL (extract, transform, load) activity;
- Migration of all collected and stored data (including all associated objects) from the Supplier Solution to any subsequent platform on termination of the Agreement, noting that this must include the data describing the relational elements as part of the dataset being migrated.

Collection and editing

- For both school and Further Education (“FE”) establishment types, facilitate ‘in the field’ collection of property related information, including (but not limited to) photos, site plans and Surveyor condition judgements, via Mobile App.
- Allow Surveyor collection of both ‘school’ and ‘FE’ establishment type data, where the data points collected differ.
- Validate inputs into the Supplier Solution against defined rules (see Appendix H: Validation Rules, for details).

Storage

- Meet current and anticipated demand for storage and processing;
- Scale to meet the likely increase in the school estate (with the associated increases in data and artefacts).

Audit

- Allow Audit of data by dedicated audit teams using functionality within Web-App.

Analysis, viewing and data sharing

- Provide reporting capability to enable analysis and further consumption of data;
- Provide a mechanism for creation and sharing of reports containing approved data with schools, responsible bodies and other users.

Interoperability and Data Export

- Facilitate seamless export of hosted data to DfE servers and systems via DfE API gateway (EAPIM).

Overarching Requirements:

In addition, the Supplier Solution must provide the following overarching requirements:

- Provision of permissions-based access to users according to role and in some cases organisation;

- Facilitate the backup and archiving of data as part of a business continuity strategy;
- Meet the defined service availability requirements;
- Be capable of being adapted to meet any changes in business need as the CDC2 Programme develops.

1.3 FUNCTIONAL REQUIREMENTS

1.3.1 FR001: User Authentication

User access to the Supplier Solution must be provisioned via currently supported web browsers and mobile, client-side applications, where end users can be authenticated. See *NFR023 Authentication (General) and DfE Sign-In Integration* for non-functional authentication requirements.

Each user of the Supplier Solution **must** be able to use a single name and password to access both Web-App and Mobile Apps. Some individual Surveyors may collect data for more than one SO; in this situation a single set of user credentials (user name, password) **is required** for Web App and Mobile App access rather than multiple credentials.

DfE Sign-In provides self-service password reset capability. If not using the DfE Sign-in provision, the Supplier Solution **must** provide the functionality for users to easily but securely reset their passwords without human support (i.e. 'Self Service' reset functionality). See *NFR023: Authentication (General) and DfE Sign-In integration* for more context.

All users **must** be authenticated and authorised to access data, function and services based on the business need and as defined by their role based user permissions (see *FR002: Permissions Based Access and User Account Management* and *Appendix A: User Permissions and Access to system functionality*).

Supporting references:

1.3.2 FR002: Permissions Based Access and User Account Management

Different user groups, defined by the DfE, **must** have access to different Supplier Solution functionality and associated data depending on their role. Data and functionality **must** be accessible to users to varying degrees including (but not limited to):

- some users having read-only access;
- some reports only being available to certain users;
- some users having account creation privileges (including the ability to set up and define permissions for users and the 'roles' to which they belong).

Some key examples of required access permissions are:

- A school user must only be able to view and download data (‘reports’) once that data has been cleared for report release. They must not be able to see data that has not be cleared, nor comments or flags on errors left by Surveyors and auditors during the audit process. They must only be able to see their own school’s data and / or reports, and not that for any other school;
- A responsible body user must only be able to see released data, but must be able to access that data for every school for which it is responsible. A local authority, for example, must be able to view all of its schools’ reports, but not those of any other responsible body;
- An SO user (regardless of role) must only be able to view data and information relating to schools that they have been ‘allocated’ to Survey during the CDC2 programme. In other words, they must be able to view and change data held in the system which has been collected by another SO;
- A DfE client superuser/admin **must**
  - have full read/write/create access to all client areas of the Supplier Solution;
  - have the ability add, remove and change permission level for all client users and roles;
  - Have the ability to define report user permissions i.e. which reports are viewable and runnable by specific user groups;
  - Be able to access all relevant system logs / reports (including but not limited user log in activity, report generation activity, data change activity).

Commented [JW1]: not

See *Appendix A: User Permissions and access to system functionality* for a full break down of roles, user groups and responsibilities.

Supporting references:

1.3.3 FR003: User Self Service support

This requirement is different to the provision of a service desk offering first line support for application related incidents, as per *SM004: Incident and Problem Management.*

Users need to have easy access to useful supporting information when using the Supplier Solution (both Mobile App and Web-App) as needed. Help and support **should** be relevant to those using it and support teams in operational delivery. All aspects of the Supplier Solution that require human interaction **should**, by design, limit the amount of human support required, but be able to facilitate it when needed.

The Supplier Solution **must** provide (but not be limited to):

- Task context specific tool-tip / hovertext like functionality to guide users’ navigation and use of both the Mobile App and Web-App components (e.g. a description of the input required from Surveyors when collecting data via Mobile App);

- Configurability of tool-tip content to be relevant to the CDC2 Programme;
- Quick user access via the Supplier Solution to relevant guidance documentation, including the ability to host or link to CDC2 Programme specific PDF format guidance created by the DfE;
- Accessibility to support and guidance that is specific to user role. For example, DfE admin level users should have access to guidance relevant to the functionality they have access to, but client end users (schools in this case) should have pared down guidance specific only to their areas of Supplier Solution use.

User guidance documentation **must** be provided by the Supplier covering (but not limited to):

- Guidance for accessing the Web-App and Mobile App components;
- Guidance for navigating the Web-App;
- Guidance for entering data (Web-App and Mobile App);
- Guidance for generating reports (Web-App).

Note: this requirement does not cover user account password self-service recovery (see *FR002: Permissions Based Access and User Account Management* , nor provision of first line support desk (see

SM004: Incident and Problem Management).

Supporting references:

1.3.4 FR004: CDC2 Process and Data Collection Workflow, Assigning and Notifications

The Supplier Solution **must** provide 'assigning and notification' functionality to users. Primarily, this functionality is used to assign a school or FE site Survey or data at different stages in the CDC2 Process to various users for completion, updating, editing, plus audit and correction, and notifying them when this happens.

- The Supplier **must** engage with the DfE during the Implementation Period to configure assigning and notification functionality. Changes to notification configuration may also be required mid-programme.
- Notification **should** occur via email to a user's account address, and **should** contain a link to the Web Portal component to allow users to 'click through', preferably directly to the section within the Web Portal related to the notification.
- Notification **should** also occur within the Web-App via pop up or equivalent message notification.
- Different user roles **must** be able to 'assign' and trigger notifications as described in (but not limited to) the table below:

CDC2 Process Stage	Name	User activity	Notifications required during or at conclusion of stage
Stage 1	Mobilisation and Planning	DfE assign site to Surveying Organisation	Notification to SO PMO that site has been set up and reference data added.
Stage 2	Pre Site Visit	SO PMO assign site to Surveyor. SO PMO schedules pre site visit meeting (Skype) SO PMO generates blank survey.	Notification to Surveyor that they have been allocated a site for Survey. Notification to Surveyor that blank site data collection survey has been created and issued to mobile device.
Stage 3	On Site	Surveyor completes data collection and 'submits' data.	Notification to SO PMO that on site data collection has been completed by Surveyor.
Stage 4	SO Quality Assurance	SO assigns Survey to SO audit within Audit Functionality. Upon completion, SO PMO assigns Survey data 'SO Approved' status.	Notification to SO Surveyor that Survey is being audited by SO PMO Audit / quality team. Notification to TQM that SO PMO has completed their quality assurance checking of a Survey's data.
Stage 5	TQM Audit	TQM chooses Survey for audit. TQM 'passes' a batch of sites or a site.	Notification to SO PMO and specific TQM audit team user that a site has been selected by the TQM for audit. Notification to DfE that a site, or a batch of sites, has successfully passed the TQM audit process.
Stage 6	Data Release	DfE marks Survey as 'released'.	Email notification automatically sent to schools and responsible bodies with link to their data reports.

Example 1 (Stage 2):
Using the Web App, a Surveyor has particular establishment's blank Survey 'allocated' to them by the SO PMO before the Survey site visit. They receive an automated notification of this to their registered email address. The Surveyor will then be able to complete this and all other Surveys allocated to them using the Mobile App whilst on-site.

Example 2 (Stage 5):

Using the Web-App, when a completed Survey has been selected for audit, that 'audit' is then allocated to a specific audit team member to review by the central audit team PMO. The audit team member receives an automated notification of this to their registered email address. Using the Web Portal, the audit team member will be able to view and progress the audits assigned to them (see also *FR007 Integrated Audit Functionality, commenting and flagging*).

The detailed description of the CDC2 Process / workflow and its delivery are located in *Appendix E: CDC2 Delivery Process* and *Appendix D: Data Status & CDC2 Delivery Process Stages.*

Supporting references:

1.3.5 FR005: Surveyor data entry, survey locking, and data editing

The Supplier Solution **must** allow data entry by users. Data entry will occur at a variety of stages of the data collection process and will involve input through a variety of different devices (both mobile and 'desktop' based) with varying levels of access for different user types.

The Supplier is not asked to provide mobile device hardware on which to run the Mobile App. Please note that automated rules based validation of inputted data is covered under *FR006: Data validation*.

The Mobile App:

- **Must** allow collection of data whilst offline i.e. without internet / data connectivity;
- **Must** allow Surveyors to input data across all specified data points labelled "SO Input" in Appendix B: Draft CDC2 Data Proforma
- **Must** allow collection of the following data types from within the Mobile App:
  - Text
  - Numbers
  - Dates
  - Photographs taken using mobile device
- **Must** allow collection of data against two main collection templates ("school establishment" and "FE establishment"). Schools and FE establishment data points are different; refer to *Appendix B: Draft CDC2 IT Data Points* for further details;
- **Must** present data fields for entry in an order defined by the DfE, in a clear and easy to understand way, and be able to split a Survey into sections on the mobile device screen to allow for validation against each section where required (see *FR006: Data validation*);
- **Must** allow a Surveyor to select values from pre-defined reference data rather than require them to manually input every time (see *Appendix B: Draft CDC2 IT Data Points* for required 'picklist' data for each data point). Reference data picklists must also apply in the Web-App service element;

- **Must not** allow Surveyors to edit or add new values to reference data pick lists whilst they are inputting data;
- **Must** allow Surveyors to add new 'blocks' and other metadata from the mobile device whilst on site and via the Mobile App;
- **Must** be able to upload data collected by Surveyors to the Supplier's main database for subsequent viewing in web-portal component either immediately upon completion of the data collection, or as soon as the Surveyor returns to a location with data connectivity (cellular data or wi-fi). Ideally this will be an automatic process triggered by completion of data collection by the Surveyor;
- **Must** allow periodic automated 'autosave' functionality during the data collection process, to avoid the potential for data loss in the event of device or Mobile App failure;
- **Must** validate inputted data during the on-site collection process (see FR006: Data validation).

Large establishments will be visited by multiple Surveyors to make data collection efficient. The Supplier Solution:

- **Must** allow multiple Surveyors to collect data about a single establishment simultaneously.

Although the bulk of data input will occur 'in the field' by Surveyors, it must also be possible for users with the appropriate permissions to be able to amend data that has already been collected and input missing data where required. For example, SO data quality teams will need to be able to review the data collected by their Surveyors and make amendments to the data if errors / quality issues are identified. The Web-App component:

- **Must** allow entry and amendment of data by users of appropriate permissions via the Web-App.

The Web-App **should** also provide functionality that allows users with appropriate permissions to amend data in bulk. For example, an auditor may discover that SOs have consistently misinterpreted a specific Survey question and have entered incorrect responses as a result, impacting a large number of school Surveys. In this situation there is a need to easily change all instances of a specific value in a field to another value across a defined list of schools, e.g. change all "0"s to "1"s for the relevant question; this **should** be achievable without having to manually edit the individual field within each Survey separately.

System wide data integrity **must** be maintained following any bulk edits of data, and validation rules in place **should** still be checked as data is changed. In the event that a bulk edit causes breaches of validation rules on either the data changed or any data relating to it, the Supplier Solution **should** inform the user of the data impacted and ask them to confirm the bulk data change before committing those changes. Any changes to the data made using a bulk edit facility **should** leave an audit trail (see *NFR010: Audit*).

The Web-App **should**:

- Allow for bulk edits to data whilst preserving data integrity and quality;

- Present to the user making the change any validation and or data integrity issues that the proposed change might cause, before the change is made.

To preserve data integrity and prevent data versioning conflict issues in general, the Supplier Solution:

- **Must** prevent editing or entry of Survey data via the Web-App whilst data is being collected via the Mobile App.

Supporting references:

1.3.6 FR006: Data validation

The Supplier Solution **must** validate the content and form of data using configured sets of rules defined by the DfE in order to maintain a high level of data quality and consistency across the CDC2 Programme.

An example of a validation rule would be that a block must always have a floor structure recorded. If no data is input against a construction type under the 'floor structure' sub element, the data capture application will not allow the Surveyor to "complete" that section of the Survey (or the CDC2 Programme assessment overall) until a floor structure construction type has been input. Furthermore, where this input might be linked to other fields (in the case of floor structure where such has been selected), the data capture application will then require that data relating to a 'floor construction finish' construction type must also be input.

Different validation rule sets may apply to different types of sites or blocks. Example 1: a limited number of unusual sites and / or blocks (defined by the DfE) may require most or all standard validation rules to be switched off to allow for data collection to take place. Example 2: FE colleges will have a different set of validation rules applicable than a school site. Separate 'sets' of validation rules must therefore be applicable to sites to accommodate this variation in site characteristics.

Appendix H: Validation Rule Works Examples provides some worked examples of validation rules required and should be considered with this functional requirement.

Validation functionality provided within the Supplier Solution **must**:

- Provide the facility to apply different sets of validation rules to different sites / blocks as appropriate;
- Check data at the point of entry within by Mobile App and Web-App against DfE defined rules, including but not limited to the following rule types:

Point of entry validation rule type	Description

‘Mandatory Field’ validation	Mandatory input of data required against the field.
‘Data-type’ validation	Restricts input to string, integer, percentage, date etc data types as required.
‘Range’ validation	Input within a numerical range.
‘Reference data’ validation	Selection from pick list only; other values are not allowed.
‘Conditional’ validation	Validation based on the content of another field or fields. Example: if [No. storeys] >1 then [GIFA] cannot be <= [Ground Floor Area].
‘Composition’ validation	Require % or integer values across several fields to sum to 100 (or a given value).

- Allow multiple point of entry validation rule types to apply to a single data field;
- Check all required mandatory data points have been completed at different stages in the data entry process, including (but not limited to) the following:

Stage based validation rule types	Description
‘Section level’ validation	Validation which prevents marking of a Survey section (as presented on the Mobile App) as ‘complete’ by Surveyors unless all required fields within that section satisfy individual field level validation rules. The Surveyor will not be able to proceed to the next section within the Mobile App unless the validation has been satisfied.
‘Survey level’ validation	Validation which prevents marking of an entire Survey as complete by Surveyors or SO PMOs until all validation rules across all fields within the Survey have been satisfied.

- Be configurable to the extent to allow amendment, addition or removal of new validation rules at any point during the CDC2 Programme, without requiring substantial development or configuration time from the Supplier;
- Where data fails validation checks, the Supplier Solution **must** notify the user through the UI of details of the field corrections or entries that are required. For example:
    - “Element 1.4. [Stairs] must be completed if [number of Storeys] is greater than 1”
- Allow for implementation of both hard and soft validation rules defined as:
    - Hard validation – validation which prevents users from entering particular data, with no exceptions;
    - Soft validation – validation which provides a warning to the user before allowing them to confirm the entry of the data.
- Allow for validation rules to be turned off for a particular Survey or subset of Survey data points, where required by the DfE. This will allow collection of data for complex or unusual sites (defined by the DfE) where validation is not appropriate.

Supporting references:

1.3.7 FR007 Integrated Audit Functionality, commenting and flagging

A formal data Audit process is fundamental to maintaining high data quality across the CDC2 Programme. Audits are the responsibility of the TQM organisation. In terms of process, Survey data is collected by Surveyors (Stage 3 in CDC2 Process), checked and audited by their own quality assurance teams (Stage 4), and then passed for formal Auditing by the TQM audit team (Stage 5).

Audits work at two levels: they take place at individual Survey level and across batches of Surveys. The quality of data across a batch will need to be checked and provide 'pass/fail' type information 'in aggregate' across that batch of Surveys (e.g. number of Surveys failed, % of failed Surveys within the batch). If the aggregate error rate across all Surveys within the batch breaches a quality threshold, that batch is then 'failed' and all Surveys held by the pending correction of the errors by SOs.

The Supplier Solution functionality to provide this is termed 'Integrated Audit Functionality'. This requirement is separated from data entry to emphasise that some Audit Functionality users may not have the ability to edit school Survey data but must have the ability to add comments or flags on the data in the system in support of the Audit process.

The Supplier Solution **must** provide a workflow and associated UI elements to allow TQM and SO Audit team users with appropriate permissions to process Audits of CDC2 Survey Data. Integrated audit functionality **should** include (but is not limited to):

- Provision of information to the Auditor on the existence of and quality of data in defined critical fields within an individual Survey (and against defined quality standards) to progress an Audit;
- The ability for an Auditor to record instances of missing Survey data;
- Provision of information to the Auditor on the existence and quality of data across a defined batch of Surveys;
- The ability to push Survey data through an audit 'workflow' whereby 'surveys' (completed sets of data) are passed between Surveyors and auditors for comment and correction;
- The ability for audit and Surveyor users to make comments on individual data points during the audit process, to describe why a data point does not meet required quality levels;
- The ability for an auditor to 'pass' or 'fail' an individual Survey;
- The ability to define 'showstopper' items within a Survey which automatically cause that Survey to 'fail' an audit;
- The ability for an Auditor to define and 'pass' or 'fail' a batch of Surveys, based on the relative quality of the Surveys within that batch;

- The ability to generate reports using the Supplier Solution on overall quality of data within a Survey (including, but not limited to, number of Survey Audit pass / fails across a given period) (see *FR011: Report creation, viewing and downloading and evidence item export*);
- The ability to give only users with appropriate permissions access to integrated audit functionality within the Supplier Solution (see *FR002: Permissions Based Access and User Account Management.*

Supporting references:

1.3.8 FR008: Data Entities, Data Collection Workflow and Data Status

Data Entities

The Supplier Solution **must** host and store data for both school and FE establishments in such a way so as to allow representation to the user of different data entities within the Supplier Solution as per the high level Entity Relationship Diagram at *Appendix I*. These include, but are not limited to:

- Provider / Establishment
- Site
- Block
- Element
- Sub-Element
- Construction Type
- Survey
- Audit
- User
- Evidence items

Each survey **must** store 'evidence item' data against different levels of collected data, e.g. Site plans at 'site level', block photo at 'block level' and condition photographs and element / construction type level. The high level ERD is provided at Appendix I provides more context. Note: storage requirements are covered under *NFR001: Scalability*.

The Supplier Solution **must** also:

- Allow the use of specific DfE defined unique references across entities to allow effective comparison of CDC2 Programme data to CDC1 data by the DfE (analysis and modelling is undertaken outside of this Agreement and is not part of this requirement). Unique references which must be used are:

Entity	School Survey data	FE Survey data

Establishment reference number	Six digits (000001, 000002 etc)	Six digits (000001, 000002, etc)
Establishment Name	URN & Estab Name & Programme name e.g. "100005 Thomas Coram Centre (CDC2)"	URN & Estab Name & Programme name.
Site reference	EFA1, EFA2, EFA3…	FE01, FE02, FE03…
Block reference	EFAA, EFAB, EFAC …EFBA, EFBB, EFBC	FEAA…FEAB
Responsible Body	TBC by the DfE	n/a

Data Status

As a Survey and its data progresses through the CDC2 Process, the Supplier Solution **must** assign a 'status' against the data reflecting the stage that the data has reached based on previous user action triggers such as a Surveyor 'completing' on site data collection. *Appendix D: Data Status and Delivery Process Stages* maps the 'status' to the relevant stage in the CDC2 Process.

The Supplier Solution **must**:

- Enable users to easily tell where a Survey's data is in the CDC2 Delivery Process, with the attribution, display of and ability to report against a data 'status' at each major point within the data collection process, including but not limited to the following:

Data status	Description	Status assignment trigger
"Imported Data"	Legacy data for an establishment that has been imported but has not yet been made available to SOs, nor the establishment surveyed (CDC2 Delivery Process Stage 1)	Initial provider set up within the Web-App, including import or ingestion of legacy data and provider metadata.
"Pre-SO Checked Data"	A site Survey has been completed by the Surveyor, and Survey fields populated, but these have not yet been quality assured / checked by the SO PMO (CDC2 Delivery Process Stages 2 and 3)	Completion of on site data collection.
"SO Approved Data"	The SO PMO has quality assured the data collected by the Surveyor and has marked it as ready for potential TQM audit (CDC2 Delivery Process Stage 4).	Completion of SO quality checking / SO audit.
"Data in TQM Audit"	Data which is being audited by the TQM. (CDC2 Delivery Process Stage 5)	Commencement of TQM audit process.
"Ready to Release Data"	Data which has passed the TQM audit process and is now ready to release to schools. (CDC2 Delivery Process Stage 5)	Successful conclusion of TQM Audit process.

Released Data	Data which has been released to schools and responsible bodies. (CDC2 Delivery Process Stage 6)	Release of data to schools using batch release functionality.

- Provide the ability to restrict access to data at certain 'statuses' above to users with the appropriate permissions only (e.g. schools should not be able to see any data with a status prior to 'Released Data');
- Facilitate the comparison of data at one status with the same data at any previous status.
- The Supplier **must** engage with the DfE during the Implementation Period to configure the how the system tracks and records travel through the CDC2 Process, and all associated status attributes and notifications. Changes to this configuration may also be required mid-programme.

Supporting references:

1.3.9 FR009 Data Sourcing, Reference Data and Legacy Data

The Supplier Solution needs to source data from a number of internal DfE data repositories. The related Non Functional Requirement provides a high level technical overview of the DfE's API gateway and is covered in *NFR007: Systems Integration*.

Reference Data

The Supplier Solution **must**:

- Allow straightforward import of Reference Data (defined as the data that defines the permissible values entered into other fields) during the Implementation Period;
- Reflect imported reference data within both the Web-App and Mobile App;
- Provide a mechanism for amending, adding or removing reference data should the operational need arise during the life of the CDC2 Programme.

Appendix B: CDC2 IT Data Points shows provides information on 'pick list' reference data in "IT Rules" columns. Note: School and FE data include different reference data.

Legacy Data

Legacy data from the previous CDC1 programme also needs to be imported or otherwise ingested into the Supplier Solution. Regardless of when it is imported / ingested, legacy data **must not** be made available via the Supplier Solution to SOs until prior to the commencement of each Tranche.

Reference data comprises:

  - CDC1 site plan (both PDF and DWG versions)

  - CDC1 Provider: establishment level metadata (establishment name, unique reference)
  - CDC1 Provider: site level metadata (site reference)
  - CDC1 Provider: block level metadata (block reference)

Data points CD01 to CD07 in *Appendix B: CDC2 IT Data Points* ("establishment level" sheet) are to be populated from Legacy Data.

The Supplier Solution **must**:

- Allow straightforward import / ingestion of Legacy CDC1 data, which includes (but is not limited to):
  - CDC1 site plan (both PDF and DWG versions)
  - CDC1 establishment metadata (establishment name, unique reference)
  - CDC1 site level metadata (site reference)
  - CDC1 block level metadata (block reference)
- Allow imported / ingested data to be mapped to CDC2 Programme establishment record sets using defined unique references.

Establishment Meta-data

Up to date information on establishment name, unique DfE reference number and other metadata is maintained within the DfE's estate. This data is used to ensure CDC2 Programme establishment meta-data is up to date throughout the CDC2 Programme.

The Supplier Solution:

- **Must** be able to ingest the following data points from the DfE's systems via API and where required update, without manual intervention, the appropriate establishment meta-data points held in the Supplier Solution:
  - School name
  - URN
  - Headteacher first name
  - Headteacher last name
  - Local Authority
  - LA Code
  - Establishment Number
  - Type of Establishment
  - Establishment Status
  - Reason Establishment Closed
  - Close Date
  - Phase of Education

- Boarders
- School Capacity
- Number of Pupils
- UKPRN
- Street
- Locality
- Address
- Town
- County
- Postcode
- Diocese
- Trust Name
- Telephone Number
- Region
- FE Establishment Type
- Last changed date

Note: *Appendix B: CDC2 IT Data Points* contains a list of all required data points; those labelled 'GIAS' in the "Source" column are those referenced by this requirement.

- **Should** be able to retrieve the above establishment meta data on a weekly basis, or on a frequency to be agreed with the DfE during the Implementation Period;
- **Must** retrieve data from DfE's systems without manual intervention;
- **Must** automatically match the data ingested via API (or other mechanism) to the appropriate record set already held within the Supplier Solution.

Supporting references:

1.3.10 FR010: User Dashboarding

Presentation of thematic information to the user via dashboard interface helps users see information relating to their role and activities in one place. The dashboards themselves do not need to be configurable by the DfE but the Supplier **must** engage with the DfE to agree detailed dashboard functionality during the Implementation Period.

The Web-App component of the Supplier Solution:

- **Must** be able to present summarised information to users in a dashboard format;
- **Must** ensure user access to specific dashboards can be configured by user role permissions (i.e. some dashboards should be hidden to some users);

- **Should** be able to summarise or otherwise aggregate data for dashboard presentation within (but not limited to) the following data boundaries:
    - user specified range of dates
    - user specified group or range of establishments
    - a specific SO's data
    - user specified data 'status' values (see FR008: Data Entities, Data Collection Workflow and Data Status).

Examples of dashboard content include (but are not limited to):

User type / role	**Dashboard content (including but not limited to)**
DfE PMO	Overall CDC2 Programme progress (sites visited, Surveys completed, reports released) across all three SOs as well as broken down by SO.
3x SOs PMOs	Number of schools allocated to SO, schools visited, Surveys completed, audited, and released.
TQM Audit Team	Dashboard within the Audit Functionality displaying key audit information such as number of audits in progress, number of pass/fails, etc.
Schools	'Survey status', date of visit, named SO contact, hyperlink / access to published report.
Responsible bodies	No. Site visits scheduled, No. Site visits completed, No. Site visits remaining, No. Reports released to date

Supporting references:

1.3.11 FR011: Report creation, viewing and downloading, and evidence item export

Users will use the Web-App element of the Supplier Solution to run reports that are both standardised and bespoke.

This functional requirement is different from viewing data within the Supplier Solution, as the data contained in a report must be downloadable by the user – the main purpose of reporting functionality is to:

- Allow the DfE to share released data with schools and responsible bodies in a pre-defined format determined by the DfE. The requirements for the report release mechanism / process is detailed in *FR012: Batch Report Release;*
- Provide downloadable information for use by the TQM and SOs to support their delivery of the CDC2 Programme e.g. Audit reports, programme pace of delivery / progress reports.

The reporting functionality provided by the Supplier Solution **must**:

- Allow reports to be accessed, generated and downloaded by users with appropriate permissions;
- Allow access to reports to be configurable by the DfE based around:
  - user role permissions
  - data status (e.g. "released")
  - individual establishment or responsible body (a school must only be able to access its own reports, and not those of any other school);
- Provide a straightforward way for schools, FE Colleges and responsible bodies to access their reports (i.e. with a minimum or user interaction with the Supplier Solution);
- Make reports available to users to download within a reasonable timeframe;
- Be capable of generating reports which can be exported in MS Word, Excel and PDF file formats;
- Allow reporting on the themes including (but not limited to):
  - Data sharing status for every school, including date of release
  - Data quality and outlier reporting
  - Condition data (Word/pdf and Excel)
  - Programme MI data (progress, KPIs)
  - User account administration activity (account creation and removal, permissions settings)
  - User account activity
  - Data audit trail (i.e. details of changes made to any given data point and by which user);
- Allow report templates (Word/PDF and Excel) to be created within the Web-App component.

Commented [JW2]: of

Reports generated in MS Word or PDF format will generally be used to share data with establishments and responsible bodies, and:

- **must** be of executive quality and easy for the user to understand
- must be configurable to allow (but not be limited to):
  - Formatted tables containing data populated automatically from CDC2 Programme data;
  - Repeated table header rows where a table spreads across multiple pages;
  - Conditional formatting of cells in tables depending on content;
  - Text content of different fonts and sizes;
  - Automatically generated page numbers and headers / footers;
  - Image files, including configurable size and placement within a report, or table within a report;
  - Hyperlinks.

Reports generated in MS Excel format **must** be able to contain (but not be limited to):

- Custom column headings
- Multiple tabs containing data
- Calculated fields
- Correct data type representation (e.g. 'number' data points are held within Excel cells as numbers, rather than 'Text').

Reports generated in MS Excel format **should** be able to contain:

- Conditional formatting of cells in tables depending on content.

User download of Evidence Items

Evidence items include site photographs, condition photographs and site plans. The Supplier Solution **must**:

- Provide the facility for schools, FE Colleges and responsible body users to download all evidence items relating to their establishment(s) via a single 'export' or report generation action undertaken by the user;
- Export photo evidence items with no loss of resolution or quality from the source objects stored in the Supplier Solution (highly compressed or very low-resolution photos will not be suitable);
- Export evidence items with references or metadata attached or included in the export, to enable the user to cross reference the evidence items downloaded to information contained in an establishment's MS Word report. For example: a school user must be able to tell which site, block, condition element and construction type a photo is 'of'.

Supporting references:

1.3.12 FR012: Batch Report Release

The CDC2 Process means that reports will usually be made accessible to schools and responsible bodies by the DfE on a monthly 'batch' basis, where the underlying data has reached and been attributed 'ready to release' status.

The Supplier Solution **must**:

- Provide a 'batch release' mechanism to allow school, FE College and responsible body reports to be released or made available to the users in batches without the need to release reports individually and/or on an establishment by establishment basis;
- Automatically notify all schools/FE colleges and responsible bodies via email (to the registered user's email address) when their reports have been released / made available;
- Be able to generate a report detailing which schools and FE establishments have had their reports released;
- Automatically attribute "Released" status to the data when the batch release has been completed.

Note: in any given month, up to 1000 schools may have their data released to them in report form. This is an anticipated maximum figure; normal release volumes will be lower (300-500) but there may be occasions where batches larger than 1000 are required in order to accommodate fluctuations in the wider pace of CDC2 Programme delivery.

Supporting references:

1.3.13 FR0013 Data Export and Import Capability

The Supplier Solution **must** be able to support exporting of Survey data held in the Supplier Solution. This is different to user reporting functionality detailed in *FR011: Report creation, viewing and downloading, and evidence item export;* although Survey data must be exportable via the standard reporting functionality detailed in *FR011: Report creation, viewing and downloading, and evidence item export*, this requirement deals specifically with the ability to export Survey data, make changes, and reimport it into the Supplier Solution.

This functionality is also separate to the requirement to transfer CDC2 Programme data to the DfE via API, which is detailed in *NFR007: Systems Integration*.

It **must** be possible for users to export and amend an establishment's Survey data in Excel format and subsequently reimport that data into the Supplier Solution. This allows for efficient QA (and where required correction) of data to be undertaken outside of the Supplier Solution by SOs.

Users with appropriate permissions **must** be able to:

- Export, in manner straightforward to the user, all non-evidence item Survey data for an establishment (e.g. an individual school) into Excel format;
- Be able to easily read and understand the resulting Excel output;
- Make any required changes to the data within Excel;
- Reimport that data from the Excel file into the Supplier Solution via Web-App component.

To allow this, the Supplier Solution **must**:

- Be able to easily export an establishment's non-evidence item Survey data into Excel format;
- Be able to update data held in the Supplier Solution with the data received from the Excel file, where the data passes validation rule checks;
- Check imported data against validation rules on fields where validation exists;
- Ensure data integrity is not compromised by export and import activity. E.g. does not allow an import to be committed or partially committed if validation rule checks are failed at the point of import;
- Notify the user performing the import action where data imported fails validation rule checks.

Supporting references:

1.3.14 FR0014 Net Capacity and Schedule of Accommodation Capture, sharing and amendment

Supplementary to the CDC2 Programme and process, data may also be collected to support school Net Capacity Assessments ("NCA") and use of spaces within the school. This data is used by DfE and Local Authorities to measure and plan school places provision. Further context about this potential aspect is given in *Appendix L: Draft Scope for NCA Solution*. Potential NCA data points are shown in *Appendix B: CDC2 IT Data Points* in 'Net Establishment', 'Net Section', 'Net Space' sheets.

The Supplier Solution should provide:

- The capability to capture Survey information at a space/room level including (but not limited to) dimensions, usage and facilities (e.g. Sinks, Toilets);
- The ability to attach and/or capture floor plans of buildings/sites and record annotations/mark ups linked to space/room level Surveys;
- The ability to record Survey data for CDC2 Programme and Net Capacity as separate or integrated Survey exercises depending on DfE operational requirements. E.g. DfE may use different organisations and Survey schedules to capture CDC2 Programme and NCA information;
- The capability for responsible bodies to view, update, and submit (via spreadsheet template if required) updated NCA data;

- Calculate Net Capacity figures for each school based on the methodology described in *Appendix N – Assessing the Net Capacity of Schools;*
- Be able to transfer data to DfE systems via API.

Supporting references:

1.4 NON FUNCTIONAL REQUIREMENTS

Where Functional requirements state what the system shall *do*, the Non-functional Requirements (NFRs) state what the system shall *be*. The Non-functional requirements specifies the criteria that can be used to judge the behaviour of the Supplier Solution. Data and system security requirements are included as a subset of NFRs.

The end-to-end Supplier Solution shall:

- provide system performance to a level required for the CDC2 Programme;
- adhere to the DfE Architecture principles that are the general rules and guidelines that inform and support the way in which DfE sets about fulfilling its mission;
- support the DfE technical strategies, which define the strategic vision to guide delivery of the DfE IT and Business modernisation programmes;
- meet Strategic characteristics, or Quality goals, including reliability, portability, scalability etc., which will be used to judge the operation and performance of the Supplier Solution;
- comply with Government guidance and Policies;
- be secure, include implementation of effective risk management processes, and engage with the DSAM process;
- comply to standards, such as ISO27001 and similar.

1.4.1 NFR001: Scalability

The Supplier must provide a Supplier Solution which is scalable. This must include (but not be limited to) application, integration, queue, messaging and storage components.

- The Supplier **must** provide a Supplier Solution which must be capable of supporting at least 27,500 users at the conclusion of the CDC2 Programme, but must also have the potential to grow to support additional users to allow for potential increases in the number of schools and responsible bodies over the length of the CDC2 Programme.
- User numbers are expected to grow by up to 5000 users per quarter following completion of Implementation Period / programme go live.

		Number of users (indicative)	Number of concurrent users (indicative)
Mobile App	Surveyors	200	200
	SO PMOs	75	75
	TQM	10	10
	DfE	2	2
	Total	287	287

		Number of users (indicative)	Number of concurrent users (indicative)
Web App	Surveyors	200	200
	SO PMOs	75	75
	TQM	10	10
	DfE	25	25
	Schools	23,000 (end of programme)	500
	Responsible Bodies	6000 (end of programme)	300
	Total	27,310	1,110

- The Supplier Solution **must** be capable of handling all associated surveys, drawings, video, photos, data files and other structured and unstructured data types without any loss of performance. As a guide, the CDC1 programme delivered 13TB of data, which would be seen as a minimum data volume over the proposed CDC2 Programme.

Supporting references:

1.4.2 NFR002: Performance

The Supplier **must** ensure that all application / system / service components are performant. This includes (but is not limited to) the user interface, data processing and storage, middleware service components, APIs, batch processing (e.g. automated report release), messaging, report queues etc.

Service Performance Targets

Service Performance requirements are detailed in Schedule 2.2 (*Performance Levels*) of the Agreement. The Supplier Solution **must** be capable of meeting the target performance measures noted in column H of the spreadsheet in Annex 1 Part 1 of Schedule 2.2 (*Performance Levels*).
Where any user interactions and related processing is expected to exceed 30 seconds the Supplier Solution **must**:

- present an indication of progress to the user (e.g. through progress bar and / or ETA information) and allow them to interact with other areas of the Supplier Solution whilst processing is in progress.

Concurrent users

- The web app and Mobile App components **must** be capable of being used concurrently with no loss of performance up to the indicative number of concurrent users.

		Number of users (indicative)	Number of concurrent users (indicative)
Mobile App	Surveyors	200	200
	SO PMOs	75	75

	TQM	10	10
	DfE	2	2
	Total	287	287

		Number of users (indicative)	Number of concurrent users (indicative)
Web-App	Surveyors	200	200
	SO PMOs	75	75
	TQM	10	10
	DfE	25	25
	Schools	23,000 (end of programme)	500
	Responsible Bodies	6000 (end of programme)	300
	Total	27,310	1,110

Supporting references:

1.4.3 NFR003: Availability

The Supplier shall ensure that all Supplier Solution components are sufficiently available to the end users. The Supplier Solution **must** be available at least 99.6% of the time, 7am-7pm Monday to Friday, measured on a monthly basis.

This does not include scheduled maintenance. Scheduled maintenance periods **must** fall outside of 7am – 7pm UK time Monday to Friday. Scheduled downtime **must** be pre-agreed with appropriate notice. The Supplier's approach **should** also follow ITIL best practice (http://www.itil-officialsite.com).

The Web-App component **should** display service status details in the event of planned maintenance or unplanned outage.

Supporting references:

1.4.4 NFR004: Reliability, Resilience and Disaster Recovery

The Supplier Solution / service **must** be reliable, resilient and be able to recover from disaster / disruption in service in a secure and efficient way. The Supplier Solution **must** include back up functionality including (but not limited to) data, OS and file system(s) as applicable, to an agreed set of Service Level Agreement's ("SLA's") to be agreed with the DfE.

For the Web-App component:

- Recovery Point Objective (RPO): No more than 30 minutes' data will be lost.

- Recovery Time Objective (RTO): The system will be recovered to full service within 4 hours.

For the Mobile App and associated data transfer mechanism components:

- Recovery Point Objective (RPO): No more than 15 minutes’ data will be lost.
- Recovery Time Objective (RTO): The system will be recovered to full service within 4 hours.

The Supplier **must** be able to supply a Business Continuity and Disaster Recovery (BCDR) plan to the DfE within 40 days of the Effective Date as detailed in Schedule 8.6 (*Business Continuity and Disaster Recovery*) of the Agreement.

Supporting references:

1.4.5 NFR005: Accessibility Standards

The Supplier **must** ensure all user interface components of the Supplier Solution comply as a minimum to the following standards:

Compliance with WCAG V2.1 to ‘AA’ Standard
Compliance with ISO 9241-171:2008 (Ergonomics of human-system Interface)
Compatible with the latest versions of the following software: JAWS, Zoomtext, Dragon NaturallySpeaking and Dolphin SuperNova and able to be used without a pointing device such as a mouse.

The Supplier **must** have effective processes in place for ensuring that their Supplier Solution maintains adequate levels of accessibility.

The Supplier **must** ensure that their product does not contravene the Equality Act 2012 in any way.

Supporting references:

WCAG V2.1 details to ‘AA’ Standard: http://www.w3.org/TR/WCAG21/

1.4.6 NFR006: Usability / User experience

The user interface of all Supplier Solution components **should** be clear, simple, and easy to use. It **should** provide an intuitive service and enable users to navigate and make use of the service without reference to a manual/user guide. Users **should** be able to undertake tasks specific to their role easily with a minimum of 'clicks' or interactions. See *Appendix G – Unique User Stories* and *Appendix C – Internal Users Characteristics* for key activities undertaken by different user types and roles.

The Supplier Solution **must** make it simple for users to perform tasks including, but not limited to:

- Searching for a specific establishment's data
- Data collection using Mobile App
- Data amendment using Web-App
- Issue and retrieval of surveys and data to and from mobile device
- Access to and downloading of reports
- Creation / customisation of reports
- Audit of data (see FR007 Integrated Audit Functionality, commenting and flagging)
- Ability for DfE admin to define and grant permissions dependant on roles
- Ability to create user accounts

The Supplier Solution **must** also allow a degree of UI configurability, including but not limited to:

- 'branding' via use of the DfE logo
- The ability to configure the order in which survey questions are presented to users of the Mobile App, and split questions into survey 'sections'.

Supporting references:

1.4.7 NFR007: Systems Integration

The Supplier Solution **must** have the ability to integrate easily to other services and/or system components across both external (to DfE) and internal (to DfE) hosting environments. It **must** be possible to integrate to these components irrespective of how the services are consumed (e.g. SAAS, PAAS, and IAAS). Supplier Solution components **must** be interoperable and use open standard programmatic interfaces.

At a high level, the Supplier Solution **must** integrate with DFE APIs and the DFE Enterprise API Management platform (EAPIM) to:

- Retrieve establishment level reference data such as school URN, name and headteacher details;
- Supply CDC2 Programme data to DfE systems.

See Appendix X: CDC2 Integration High Level Conceptual Design for further technical context.

The Supplier Solution **must**:

- Be able to discover, connect and send data to DFE CDC2 API end points hosted on the EAPIM. The DFE CDC2 API will follow the OpenAPI and RESTFUL standards and the API specification will be agreed and defined in collaboration with the Supplier during the Implementation Period and afterwards shared with the Supplier in the form of OpenAPI (Swagger) definition;
- Be able to also consume the reference data via CDC2 Programme reference data api (REST) hosted on the Enterprise APIM. The reference data API would be protected by OAuth2.0 authorization protocol. The OAuth tokens can expire after certain time (normally 1 hour) and the Supplier must be able to refresh the tokens by making calls to DFE OAuth Authorization server.

The data collected as part of the CDC2 Programme is classified as “Official Sensitive” and the DfE API created to ingest the data from the Supplier will be secured by OAuth2.0 authorisation protocol.

The Supplier Solution **must**:

- be able to ensure that the application can access/make outbound calls to DFE OAuth2.0 enabled REST API on schedule, manual or event-based integration.

Data Frequency & Failures

The Supplier **should** be able to batch all CDC2 Programme data including evidence items into manageable data segments before sending it to the DfE CDC2 API and **should** be able to monitor and retry sending the data upon any failures (loss of connectivity etc.). The Survey data send frequency, batch sizes and delivery schedules should be flexible and configurable in the Supplier Solution.

Only data with the status ‘SO Approved’ (or any subsequent ‘statuses’ in the CDC2 Process) needs to be sent to the DfE CDC2 API (see *Appendix D: Data Status and CDC2 Delivery Process Stages* for list of statuses mapped to CDC Process stage). Only new or updated data should be transferred – a full data set at each transfer is not required.

The frequency of API updates to DfE systems **must** - as a minimum - be weekly; more frequent e.g. nightly ‘refresh’ frequencies are preferred.

Supporting references:

Appendix O: CDC2 API Integration High Level Conceptual Design Diagram

1.4.8 NFR008: Interoperability

The Supplier Solution **must** support the concept of ‘pick up and play’ by being available across multiple platforms (browsers and mobile apps) and multiple devices (desktop/laptop/tablet/smart-phone, etc.), with single sign-on for office-based users and secure but simple access for mobile and other windows users.

Supporting references:

1.4.9 NFR009: Management Information

The Supplier Solution **must** provide a Management Information (“MI”) reporting capability in compliance with Schedule 8.4 (*Records Provisions)* and support production of information in compliance with Schedule 2.2 (*Performance Levels*) of the Agreement. This **should** be provided through existing pre-built reports and dashboards, and also provide the ability for users to quickly produce their own reports.

MI Reporting **should** be:

- Easily usable and accessible
- Easily understandable and not overly complex
- Real time and/or scheduled
- Interactive and have the scalability and ability to customise to encourage use

Supporting references:

1.4.10 NFR010: Audit

The Supplier Solution **must** operate audit controls to monitor access to the service, the longevity of the audit log(s) and its completeness. There **should** be a regular audit timetable which details what the audit covers. Auditing **must** be able to monitor and record (but not be restricted to):

- Actions by users, including log in date and time and activity undertaken.
- Actions by the administrators, including log in date and time and activity undertaken
- Reports generated / accessed by users, including date of access.

The DfE’s administrators **should** have access to a range of audit reports to show which records have been updated. There **should** be flexibility in the creation and parameters of these reports. Reports **should** also be able to identify trends and risks.

Audit must be ‘always on’ and, must have no impact on the performance of the Supplier Solution.

Supporting references:

1.4.11 NFR011: Ownership and Data Access

The Supplier Solution **must** allow the DfE to legally own the business data inside the Supplier Solution, and the DfE **must** be able to gain access to it as required, as detailed in Section F (*Intellectual Property, Data and Confidentiality)* of the Agreement. Access to data by non DfE-authorised users **must** be prevented, as detailed in Schedule 2.4 (*Security Management*) of the Agreement.

Supporting references:

1.4.12 NFR012: Data Environments

The Supplier Solution component(s) **must** be made available to the DfE with test, production, pre-production and training environments.

- A Production System **must** be provided that meets all requirements.
- A Training System **must** be provided which is functionally identical to the production system but with no access to live data.
- A Test & Reference System **must** be provided that is suitable for technical integration and user acceptance testing of new versions or functionality prior to their release into the production environment.

Supporting references:

1.4.13 NFR013: Open & Digital Service Standards

The Supplier and their Supplier Solution **must** adhere to a number of standards covering ‘open’ software and digital standards generally, as detailed in Schedule 2.3 (*Standards*) of the Agreement. Note: required security standards are covered under requirements NFR019-26.

Open standards

To avoid lock-in and enable the maximum level of interoperability between products and services, the Supplier **should** provide products and services which are either based on open standards, or have the ability to support open standards (such as open source software).

The Supplier shall ensure that:

- Where possible, the Supplier Solution is aligned with the Cabinet Office guidelines on open standards (https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles
- Where the Supplier Solution cannot align to open standards then it **must** enable commonly available standards, including but not limited to XLSX and DOCX, CSV, PDF ODT, ODS and ZIP;
- The Supplier Solution **must** enable compression of large images while maintaining a usable resolution and level of details;
- The Supplier Solution **does not** impose unnecessary licence cost, or lockdown to individual service providers, caused by proprietary file formats or media codecs.

Cabinet Office Digital Service Standards

All DfE IT contracts **must** adhere to relevant Cabinet Office service standards.

The Supplier shall ensure that:

- Their Supplier Solution and ways of working are aligned with the Government’s Digital Service Standards (https://www.gov.uk/service-manual/service-standard)
- Their Supplier Solution and ways of working are aligned with the Government’s Technology Code of Practice (https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice)

Supporting references:

https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

https://www.gov.uk/service-manual/service-standard

https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

1.4.14 NFR014 Extensibility and Customisation

The Supplier Solution **must** be able to be easily adapted to support changes to the current business processes should the operational need arise. This includes but is not limited to changes to:

- Look and feel
- Data collection workflow and data entry process
- Audit workflow
- Data validation rules
- Data interoperability interfaces
- Reporting requirements

This adaptation **should** be possible via configuration rather than development.

Supporting references:

1.4.15 NFR015: Testing Approach

The Supplier Solution **must** be fully tested prior to the Operational Services Commencement Date (including initial configurations bespoke to the DfE), and prior to implementation of new functionality / software version. This is detailed in Schedule 6.2 (*Testing Procedure*) of the Agreement.

The Supplier shall be responsible for internally testing the Supplier Solution and individual components within it prior to UAT to provide confidence to the DfE that it meets all of the requirements. The Supplier **must** track the status of defects from the point of identification until they have been closed.

The Supplier **must** submit a Test Strategy to the DfE no later than 20 Working Days from the Effective Date. The Test Strategy **must** include (but should not be limited to):

- an overview of how Testing will be conducted in accordance with the Implementation Plan;
- the process to be used to capture and record Test results and the categorisation of Test Issues;
- the method for mapping the expected Test results to the Test Success Criteria;
- the procedure to be followed if a Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issues;
- the procedure to be followed to sign off each Test;
- the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for

the resolution of Test Issues;

- a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and DfE, TQM or SO involvement in the tests;
- the technical environments required to support the Tests; and
- the procedure for managing the configuration of the Test environments.

Supporting references:

1.4.16 NFR016: Fault resolution

The Supplier Solution **must** be able to deal with fault resolution in a robust and effective manner. The DfE's proposed fault categories are set out in the table at paragraph 4.5 of Part II of Schedule 2.2 (*Performance Levels*).

Supporting references:

1.4.17 NFR017: Product Roadmap

The Supplier Solution **should** have a clear product roadmap of regular upgrades to all aspects of the software which should also include a high level timeline.

The Supplier **must** provide a high-level product roadmap of the Supplier Solution components.

Supporting references:

1.4.18 NFR018: Innovation

It is important that the Supplier Solution can keep pace with technology advances and adopt these where technology innovations can improve or optimise business processes and reduce overall cost to DfE. The Supplier **should** be able to demonstrate their commitment to innovation.

Supporting references:

1.5 SECURITY

The DfE has a number of security and compliance considerations that the Supplier must be able to meet and demonstrate evidence of. These are detailed in NFR19 to 26 inclusive.

1.5.1 NFR019 Security Assurance Model

CDC2 data is classified as Official Sensitive. The Supplier Solution **must** meet or exceed the expectations set out in:

- The Authority Security Standards out in Annex 1 of Schedule 2.4 (*Security Management)*
- The Government's Minimum Cyber Security Standard (https://www.gov.uk/government/publications/the-minimum-cyber-security-standard)

The Supplier **must** hold and evidence the following:

- ISO 27001:2013 certification

Supporting references:

Government security classifications:

https://www.gov.uk/government/publications/government-security-classifications

1.5.2 NFR020 Data Security

The Supplier **must** ensure that data, and the assets storing or processing it, are protected against physical tampering, loss, damage or seizure. This can be demonstrated by adherence to the standards described.

Mobile applications **must** implement their own secure area on the device, including encryption of data held on the device. Mobile applications **must not** allow material stored within the secure area to be copied to an insecure area or off the device (except when uploaded into the Web-App component during the survey upload process).

Supporting references:

Data Centre Security:

CSA CCM v3.0

SSAE-16 / ISAE 3402

Data at Rest:

https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

Further information on satisfying this requirement can be found here: https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience

1.5.3 NFR021 Security Vulnerability Management

The Supplier **must** track, assess and manage information related to security vulnerabilities and threats, and operate and manage its service in order to impede, detect or prevent attacks.

Supporting references:

Vulnerabilities: ISO/IEC 30111:2013

Incident Management: ISO/IEC 27035-1:2016

CSA CCM v3.0

ISO/IEC 27001

Safecode 'Fundamental Practices for Secure Software Development'

ISO/IEC 27034

CESG CPA Build Standard

https://www.ncsc.gov.uk/guidance/cloud-security-principle-5-operational-security

1.5.4 NFR022 Continuous Assurance

The Supplier **must** ensure that:

- Annually commissioned IT Security Health Checks (ITHC) are conducted using a CHECK certified provider;
- They will share ITHC results and remediation plans with the DfE.

The Supplier Solution will be subject to DfE security assurance in accordance with the DSAM process.

- The Supplier **must** engage with the DfE during the DSAM process and supply information such as ITHC results, remediation plans as required.

The DfE will provide findings to the Supplier for response and remediation (if required).

Supporting references:

CHECK certification: https://www.ncsc.gov.uk/information/check-penetration-testing

CSA CCM v3.0

ISO/IEC 27001

https://www.ncsc.gov.uk/guidance/cloud-security-principle-5-operational-security

1.5.5 NFR023 Authentication (General) and DfE Sign-In Integration

The DfE has an identity and access management solution called DfE Sign In. The Supplier Solution **should** be able to integrate with DfE Sign In for school and responsible body users.

- DfE Sign In is an open-source product that supports both SAML2 interactions for legacy services and OpenID Connect for new services.

Note: Users which are not schools and responsible bodies such as (SOs and TQM users) will not use DfE Sign In and will need to be authenticated using the Supplier's existing authentication provision.

The Supplier Solution **should**:

- integrate to the DfE's identity and access management components ("DfE Sign-In) in a way that compliments a "single sign" on pattern and supports SAML2 or OpenID Connect interactions as outlined above.

If the Supplier is unable to integrate with DfE Sign In, all users **must be** authenticated using the Supplier's own authentication provision, not just TQM and SO users.

The Supplier **must** ensure that access to their Supplier Solution must remain secure and must not be accessed without authenticating the user. Specifically:

- All users of the Supplier Solution not using DfE Sign In authentication **must** be able to authenticate securely;
- the Supplier Solution **must** ensure all internal and external connections (user and entity) go through an appropriate and adequate form of authentication;
- assurance **must** be provided that this control cannot be bypassed;
- the Supplier Solution **must** be able to restrict access to certain functionality and data through the designation of various roles and functions;
- the Supplier Solution **must** ensure that authentication credentials do not traverse the network in clear text form;
- The Supplier Solution **must** be able to provide multi-factor authentication where required for privileged accounts ("MFA").

Supporting references:

1.5.6 NFR024 Authorisation (General)

The Supplier **must** ensure that access to the Supplier Solution remains secure. The Supplier Solution and functional areas within it **must** only be accessed by those individuals or entities with authorisation. More specifically, the Supplier Solution **must**:

- ensure that there are effective authorisation mechanisms in place, where appropriate;
- provide a secure way of enabling users to reset their passwords;
- contain clearly defined user types and permissions;
- ensure there is a least privilege stance in operation;
- ensure that the authorisation mechanisms work properly, fail securely, and cannot be circumvented;
- ensure that authorisation is checked on every request.

Supporting references:

1.5.7 NFR025 Cryptography

The Supplier Solution **must** protect data during transmission and ensure its integrity. The Supplier **must** ensure that:

- no sensitive data is transmitted in clear text, internally or externally;
- known good cryptographic methods are implemented;
- Certificates cannot be self-signed and come from established and reliable independent Certificate Authorities;
- Strong ciphers are utilised and key management process is documented;
- Data at rest is encrypted to AES256 standard, such as through TDE or Bitlocker;
- Data in transit is encrypted at TLS 1.2 or above.

Supporting references:

Further information on satisfying this requirement can be found here:

https://www.ncsc.gov.uk/guidance/cloud-security-principle-1-data-transit-protection

1.5.8 NFR026 Service Separation

The Supplier Solution **must** ensure that a malicious or compromised user of the service cannot affect the service or data of another. CDC2 Programme data **must** therefore be segregated from other customers' data within the Supplier Solution.
Supporting references:

1.6 SERVICE MANAGEMENT REQUIREMENTS

The DfE is looking to procure an end to end service to ensure that users of the delivered Supplier Solution are fully supported, post implementation. The Supplier must demonstrate the requirements set out in this section.

1.6.1 SM001: Implementation and Exit Management

Implementation

The Supplier **must** ensure that all components of the Supplier Solution are configured, user tested and fully operational within 6 months of the Effective Date to allow for Survey data collection to begin in accordance with the intended timetable for the CDC2 Programme. UAT will encompass an end-to-end test of all required functionality and will be undertaken by the TQM, SOs and DfE.

The Supplier **must** provide a detailed Implementation Plan to the DfE within 20 days of the Effective Date.

The content of the detailed Implementation Plan is set out in Schedule 6.1 (*Implementation Plan*) of the Agreement and **must** include (but is not to be limited to):

- Proposed timescales for achieving relevant milestones (e.g. build, configuration, testing, go-live, exit activities);
- Proposed steps required to achieve all relevant milestones falling within 15 months of the Effective Date;
- Proposed timescales for training and roll out activities (note: training requirements are described in *SM002: Training* and are not part of this requirement;
- Clearly outlined roles and responsibilities of the DfE and the Supplier.

Exit Management

The Supplier **must** provide an Exit Plan to the DfE within 3 months of the Effective Date. This plan will be reviewed and where required updated on an annual basis, and **must** set out the Supplier's proposed methodology for achieving an orderly transition of the Services from the Supplier to the DfE and/or any replacement supplier on the expiry or termination or the Agreement.

The Exit Plan **must** include details as laid out in Schedule 8.5 (*Exit Management*) , such as (but not limited to):

- Data to be transferred to the DfE;
- The mechanism for transferring that data;
- The mechanism for securely destroying data held by the Supplier;
- A project delivery plan;

- An outline of risks, issues and dependencies;
- Details of Supplier personnel that will be engaged in the off-boarding process, with roles and responsibilities outlined.

Note: further details on required content of the Exit Plan are detailed in Schedule 8.5 (*Exit Management*) of the Agreement.

Supporting references:

Advice on HMG secure sanitisation policy and approved methods are described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

1.6.2 SM002: Training

The Supplier **must** provide training to users of both the Mobile App and the Web-App Solution components. Training **must** cover how to undertake key tasks based on user role (see Appendix G: CDC2 Unique User Stories and Appendix C: CDC2 Internal Users Characteristics).

This is likely to be a mixture of (but will not be limited to):

- face to face Surveyor and SO PMO training (group based, at locations across England);
- virtual training;
- one-to-one training for the DfE 'super user' role.

The DfE anticipate that up to 9 days' training will be required during the CDC2 Programme Implementation Period. Further training will be required over the remainder of the CDC2 Programme to allow for Surveyor and PMO team member turnover; the Supplier **must** engage with the DfE to agree appropriate frequency for this training. Training will also be required for new Mobile App or Web-App functionality which requires a major change in process for user task completion.

Supporting references:

1.6.3 SM003: Delivery Team and Scheduled Meetings

The Supplier **must** convene a CDC2 Programme delivery team with sufficient skills, experience, resources and authority within the Supplier's organisation to effectively work with the DfE and deliver the CDC2 Programme, including during the Implementation Period.

The Supplier **must** be able to attend, as a minimum, scheduled Business As Usual ("BAU") meetings with the DfE and TQM and attend ad-hoc meetings as required.

The table of BAU meetings the Supplier is required to attend is set out in Annex 1 of Schedule 8.2 (*Governance*).

Additional non-scheduled meetings will be required e.g. for scoping and UAT reporting of new functionality, urgent issue escalation and resolution, etc.

Supporting references:

1.6.4 SM004: Incident and Problem Management

The Supplier **must** have Incident and Problem Management processes within their organisation that fully support (and are designed to meet the needs of) external customers, with a varying range of skill sets and experience.

The Supplier **must** be able to provide (but not be limited to) the following:

- A support desk function which:
  - I. Offers first line support for application related incidents, via channels such as telephone, email and Instant Message (where possible the Supplier Solution should offer online help and guidance to minimise incident volumes);
  - II. Is able to take and process incident and queries between 08:00 to 18:00 Monday to Friday (excluding Bank Holidays) indicating the provision available outside of these hours;
- a clear process, shared with the DfE, for the escalation of service related incidents, including references to how this dovetails with contractual escalation.

The DfE's proposed fault / incident categories are as set out in Schedule 2.2 (*Performance Levels*).

Supporting references:

1.6.5 SM005: Service Reporting

The Supplier **must** have Service Reporting processes within their organisations that fully support (and are designed to meet the needs of) external customers. The Supplier **should** ensure that Service Reporting outputs are provided in a clear, transparent and itemised way, where applicable.

Service reporting outputs from the Supplier will be discussed in quarterly performance review meetings between the Supplier and the DfE (see

SM003: Delivery Team and Scheduled Meetings). Reporting **must** cover (but will not be limited to):

- Metrics including but not limited to, incident, service interruption, resource usage, API throughput statistics. See *Schedule 2.2 Annex 1 Part 1 (Performance Levels)* Annex for information on KPIs the DfE intend to measure to assess system performance;
- Security incidents and potentially suspicious user account activity;
- Progress and cost reporting on any development and associated implementation commissioned by the DfE (see also *NFR014 Extensibility and Customisation*);
- Service interruption root cause, resolution and action plan to mitigate future outages of the same nature;
- Details of any proactive changes identified to maintain high performance and availability;
- Key Supplier Solution related issues and risks affecting or with the potential to affect CDC2 Programme delivery, including details of any forthcoming outages or remedial work that will affect service;
- Volume of support desk enquiries by issue category over a given reporting period, and in comparison to previous reporting periods.   Categories include (but will not be limited to):
    - Supplier Solution access
    - Report access / generation
    - UI delay / timeout

Supporting references:

APPENDICES

Appendix A - User permissions and acce

Appendix B - DRAFT CDC2 IT data points v

Appendix C - CDC2 Internal Users Charac

Appendix D - Data Status and CDC2 Deli

Appendix E - CDC2 Delivery Process V1.1.

Appendix G - CDC2 Unique User Stories.xl

Appendix H - Validation Rules Worl

Appendix I - High Level ERD.pdf

Appendix L Draft Scope for NCA solutic

Appendix N - DfES-Assessing the N

Appendix O - CDC2 API Integration High I

Note: Appendices F, J, K and M are not used.

Glossary

What follows is a glossary of abbreviations, acronyms and terms used within the context of this Schedule 2.1 (*Services Description*):

Abbreviation	Term	Description
CESG	Communications-Electronics Security Group	is the UK government's National Technical Authority for Information Assurance. The website is http://www.cesg.gov.uk/Pages/homepage.aspx
CSV	Comma Separated Values	A flat file format where data values are separated by a comma character.
DMZ	De-Militarised Zone	DfE have a number of DMZ environments to protect the secure 3DC hosting environment from incoming data transfers.
DR	Disaster Recovery	DR involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity
DSAM	Departmental Security Assurance Model	The key features of the DSAM are: ▪ The Security Assurance Model provides a clearer roadmap for a project to be initiated, risk assessed, controls identified and its security assurance measured and tested. It will be embedded within the Stage Gate process and will allow the business to gain appropriate and proportionate security assurance for its systems, services, applications and network solutions. ▪ The Security Assurance Model contains a number of pre-defined tools and documents to aid the business in achieving an appropriate level of security assurance. ▪ DSU owns and maintains the model, but it will be operated by the business and projects.

Abbreviation	Term	Description
DSU	Departmental Security Unit	The DSU is responsible for ensuring that appropriate security arrangements are in place to help DfE employees and others with authorised access to DfE systems carry out the DfE's business to comply with HMG Standards.
ESFA	Education and Skills Funding Agency	The Education and Skills Funding Agency (ESFA) is responsible for distributing funding for state education in England for 3-19 year olds, as well as managing the estates of schools and colleges.
FE	Further Education (sector);	The FE sector provides education in addition to that received at secondary school, that is distinct from the higher education (HE) offered in universities and other academic institutions.
HMG	Her Majesty's Government	
HTTP	Hyper Text Transfer Protocol	HTTP is the foundation of data communication for the World Wide Web.
ICT	Information and Communications Technology	means Information and communications technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end Supplier Solution
IEx	Information Exchange	ESFA's external customer portal which is hosted in CCI and built on open source software.
ISO 22301		is the International Standard describing for Business Continuity
ITIL	Information Technology Infrastructure Library	a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business
LA	Local Authority	UK's lowest level of public administration.
MAT	Multi-Academy Trust	A trust governing 2 or more academy schools in England.
MS	Microsoft	US software services provider.
MTTR	Mean Time To Recover	The average time it takes for the Supplier to restore a service.

Abbreviation	Term	Description
PDF	Portable Document Format	Each PDF file encapsulates a complete description of a fixed-layout flat document, including the text, fonts, graphics, and other information needed to display it
PDS, PDSP	Property Data Survey Programme	The PDS was the previous condition data programme to the Condition data Collection.
PMO	Project Management Office	The teams within the Authority and Supplier responsible for project and programme management.
PSN	Public Service Network	PSN is a UK Government programme to unify the provision of network infrastructure across the United Kingdom public sector into an interconnected "network of networks" to increase efficiency and reduce overall public expenditure.
RB	Responsible Body	A DfE&ESFA term for those that have oversight of capital maintenance and financial matters for schools under their jurisdiction. RBs include Local Authorities, Dioceses, MATs and individual Free Schools.
RPO	Recovery Point Objective	Acceptable amount of data loss (as expressed in time)
RTO	Recovery Time Objective	Acceptable time for the service to be restored
SAML	Security Assertion Markup Language	Works by transferring the user's identity from one place (the identity provider) to another (the service provider). This is done through an exchange of digitally signed XML documents.
SCAP	Schools' Capacity Survey	Schools' Capacity Data captured via the DfE Data Capture portal and processed before being stored in The Store
sFTP	Secure File Transfer Protocol	A network protocol that provides file access, file transfer, and file management over any reliable data stream
SIRO	Senior Information Risk Owner	The DfE's most senior risk owner in relation to data and information.
SIRA, CCP SIRA	Security and Information Risk Advisor	the Security and Information Risk Advisor (SIRA) is a role defined under the CESG CESG Certified Professional Scheme, who reports to the SIRO. SIRAs undertake DSAM assessments.
SLA	Service Level Agreement	Support and performance-related requirements

Abbreviation	Term	Description
SPF	HMG Security Policy Framework	This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.
TDA	Technical Design Authority	Provides technical assurance for projects throughout their lifecycle. It achieves this by conducting Technical Assurance Reviews in designated lifecycle stages as a requirement of authority to proceed through the associated stage gate
UAT	User Acceptance Testing	Is a phase of software development in which the software is tested in the "real world" by the intended audience.
WCAG	Web Content Accessibility Guidelines	WCAG is a series of web accessibility guidelines published by the Web Accessibility Initiative (WAI) of the World Wide Web Consortium (W3C), the main international standards organization for the Internet. They are a set of guidelines that specify how to make content accessible, primarily for people with disabilities—but also for all wcag agents, including highly limited devices, such as mobile phones
XLSX		is a zipped, XML-based file format developed by Microsoft[3] for representing spreadsheets, charts, presentations and word processing documents
XML	Extensible Markup Language	A set of rules for encoding documents in a format which is both human-readable and machine-readable. It is defined by the W3C's XML 1.0 Specification and by several other related specifications, all of which are free open standards.
	Cyber Essentials, Cyber Essentials Plus	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.
	Digital Marketplace / Gcloud	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.

Abbreviation	Term	Description
	Penetration Testing	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.