ELTO Employers' Liability Tracing Office

ELD NextGen

Frequently Asked Questions

8th October 2026
Version 1.4

Purpose of this Document

This document provides answers to questions raised by insurers and delegated authorities about the ELD NextGen policy management changes.

It consolidates feedback and questions raised through workshops, webinars and direct engagement sessions. This document will be updated regularly as further detail is confirmed, including API documentation, transition planning, portal registration and cutover arrangements.

Where information is not yet final, this is marked as *to be confirmed*.

Key terms

Term	Definition
API	An Application Programming Interface. In this context, the API is the system-to-system route used to submit policy data to the ELD.
Direct API submission	A submission where policy data is sent directly in the API request body.
API file upload	A submission where a file is uploaded through a secure API-led process.
Policy key	The set of fields used to uniquely identify a policy record. Previously known as the Compend, Compound or Composite key. This is not a physical field in the ELD but derived from the fields that make up the key.
Supplementary policy reference	An optional reference that forms part of the policy key when provided. Previously known as the BrokerDARef.
Parent / child hierarchy	The current ELD structure where a parent policy may have one or more child policies. This hierarchy is being removed in the new model.
Single policy record	The new structure where a policy contains all covered employers at equal standing.
Adjusted employer cover dates	Employer-level dates used where a specific employer's cover period differs from the overall policy cover period.
CRN	Company Registration Number. This field is optional.
ERN	Employer Reference Number.
Status endpoint	The API endpoint used to check the processing status and validation results for a submission.
ELD policy management area	The area of the ELD portal where users can manage policies and view submission status and validation results.

Contents

1 About the Change 3

2 Timeline, Transition and Cutover 5

3 Support, Engagement & Communications 8

4 Portal Access, Registration & User Administration 11

5 Policy Data Model & Policy Key 15

6 Parent / Child Policy Changes 20

7 Submission Routes & File Formats 23

8 Validation, Errors and Submission Status 27

9 Testing, Reporting and Ongoing Operations 32

Public Domain

1 About the Change

Questions in this section

1.1 What is changing? 3

1.2 Why is ELTO making this change? 3

1.3 Is this only a technical change? 4

1.4 Which source should we treat as the authoritative technical API specification? 4

1.5 What documents should insurers review? 4

1.1 What is changing?

ELD policy data submission is moving from the existing SFTP file-drop process to a modern HTTPS API.

The new approach supports:

- direct API submission for smaller or more immediate updates;
- bulk file upload through the API;
- standard JSON and pipe-delimited text formats;
- clearer validation responses;
- improved visibility of submission status and validation results;
- a simplified policy data model.

The data model is also changing. Policies will be structured as a single policy record containing all covered employers, replacing the existing parent/child hierarchy.

1.2 Why is ELTO making this change?

The change is intended to improve the reliability, sustainability and usability of ELD policy management.

The key objectives are to:

- improve data quality;
- simplify and modernise submission processes;
- reduce operational complexity;
- provide clearer validation feedback;
- improve auditability and traceability;
- support future integration through modern APIs;
- improve visibility of submission status and errors.

1.3 Is this only a technical change?

No. Although the API is a technical change, the programme also affects business and operational processes.

Insurers should consider the impact on:

- existing SFTP submission processes;
- operational teams who review errors;
- portal users;
- delegated authority arrangements;
- data reconciliation activity;
- cutover and transition planning;
- compliance and audit processes.

1.4 Which source should we treat as the authoritative technical API specification?

The Developer Portal is the authoritative current technical reference for the ELD APIs. The downloadable OpenAPI definition describes the machine-readable endpoint contracts and schemas. The ELD Policy Schema Guide explains field purpose and legacy mapping, while the File Transfer Guide explains the pipe-delimited file format.

1.5 What documents should insurers review?

Insurers should review the Policy Management Summary of Changes and this FAQ document. For those who will be using the new API to manage policies on the new ELD should also read the ELD Getting Started Guide, ELD Policy Schema Guide and ELD File Transfer Guide. Developers should use the ELD Developer Portal for the authoritative current endpoint specification, request/response examples and downloadable API definition. Bearer-token guidance is also available in the Developer Portal.

2 Timeline, Transition and Cutover

Questions in this section

2.1 When is go-live planned? 5

2.2 Will existing policy data need to be re-supplied? 5

2.3 Will SFTP be switched off at go-live? 5

2.4 Will there be a period of tandem running between SFTP and the new API? 5

2.5 Can insurers stay on the old database beyond March 2027? 6

2.6 Will there be a detailed transition plan? 6

2.7 What does "registration and planning" mean in practice? 6

2.8 Who should insurers involve internally? 6

2.9 Can an insurer request a preferred point within the Q1 2027 cutover window? 7

2.10 How much implementation effort should insurers allow for the API change? 7

2.11 Will end-user training be provided? 7

2.1 When is go-live planned?

The target is a phased release during Q1 2027 (January – March 2027). Further detail will be confirmed in the transition and cutover plan.

2.2 Will existing policy data need to be re-supplied?

No. Existing policy data will be migrated automatically into the new platform.

Insurers will not need to re-supply existing historic policy records as part of the migration.

2.3 Will SFTP be switched off at go-live?

Once an organisation has transitioned to the new platform, its SFTP access will be revoked.

The current SFTP service is expected to be turned off from April 2027.

Details will be included in the transition and cutover plan.

2.4 Will there be a period of tandem running between SFTP and the new API?

There will be no production parallel running for policy management. When an organisation launches on the new platform, its legacy SFTP policy-management access will be revoked. Insurers will have access to a non-production Test environment in advance of go-live so integrations can be developed and tested before cutover.

2.5 Can insurers stay on the old database beyond March 2027?

Insurers are expected to transition to the new ELD platform during Q1 2027, with the current SFTP service scheduled to be turned off from April 2027.

Any readiness concerns should be raised with ELTO as early as possible so they can be considered as part of transition planning.

2.6 Will there be a detailed transition plan?

Yes. ELTO will provide a detailed transition and cutover plan.

This will include:

- key dates;
- onboarding activities;
- registration requirements;
- testing expectations;
- cutover arrangements;
- support arrangements;
- any migration or freeze windows;
- actions required from insurers and delegated authorities.

Onboarding activities (including registration, access setup and testing) form part of this plan

2.7 What does "registration and planning" mean in practice?

Registration and planning refers to the preparation activity required by insurers and delegated authorities before transitioning to the new platform.

This includes:

- confirming technical, operational and communication contacts;
- identifying current SFTP feeds and batch processes;
- deciding which submission routes will be used;
- preparing for portal user registration;
- identifying delegated authority arrangements;
- planning internal testing;
- preparing for cutover.

Further onboarding guidance will be provided.

2.8 Who should insurers involve internally?

Insurers should involve representatives from:

- policy operations;

- delegated authority teams;
- data teams;
- IT and integration teams;
- compliance and audit;
- portal user administration;
- business change or operational readiness teams.

Organisations should also identify ownership of current SFTP submissions and future API onboarding.

2.9 Can an insurer request a preferred point within the Q1 2027 cutover window?

All non-API users will transition on launch. API users will be transitioned over a staggered period following launch. Insurers should raise significant business constraints, such as audit or regulatory periods, as early as possible. ELTO can take a preferred period into consideration when planning cutover cohorts, although the final cohort plan remains subject to programme scheduling.

2.10 How much implementation effort should insurers allow for the API change?

Implementation effort will vary between insurers depending on existing systems, integration approaches, security controls and internal change processes.

As a broad guide, the technical build and testing activity may typically take around 20–40 working days for a relatively straightforward implementation, including authentication, policy submission, file handling, status polling, error handling and testing.

The overall elapsed implementation period may be longer where legacy system changes, third-party suppliers, security approvals or internal release processes are required.

2.11 Will end-user training be provided?

Yes. The platform is being designed to be simple and intuitive, and online training will be provided.

ELTO will also provide walkthroughs, guidance materials and drop-in sessions to support users before and during rollout.

3 Support, Engagement & Communications

Questions in this section

3.1 Will there be more workshops or discussion sessions? 8

3.2 Will there be technical support sessions? 8

3.3 Will there be a developer portal? 8

3.4 When will full API documentation be available? 9

3.5 Will webinar presentation and recording be available? 9

3.6 Will the slides from previous webinars be reissued? 9

3.7 How will ELTO share updates to documents and design decisions? 9

3.8 Can insurers nominate additional attendees for future webinars? 9

3.9 Can we ask questions on the API documentation once it is released? 9

3.10 How should insurers raise issues, clarifications or risks? 9

3.11 How often will ELTO provide updates? 10

3.12 Are worked examples or screenshots available for API file uploads? 10

3.13 Will insurers still have a KAU or named relationship contact? 10

3.1 Will there be more workshops or discussion sessions?

Yes. ELTO will continue engagement through webinars, workshops and drop-in sessions.

These sessions will support both business and technical audiences.

3.2 Will there be technical support sessions?

Yes. Technical support sessions are available to support API and integration questions. Please contact ELDNextGen@elto.org.uk, along with your specific questions and we will arrange a call with the right team.

3.3 Will there be a developer portal?

Yes. The ELD Developer Portal is available for authorised technical users. It provides the endpoint documentation, schemas, examples, API definition download and supporting resources needed to build and test an integration.

3.4 When will full API documentation be available?

The API documentation is available now through the Developer Portal, supported by the Getting Started, Policy Schema and File Transfer guides. The live Developer Portal should be checked for the current version.

3.5 Will webinar presentation and recording be available?

Yes. Webinar materials will be made available after each session.

Details of how to access recordings and presentations will be shared with attendees.

3.6 Will the slides from previous webinars be reissued?

Yes. Webinar slides will be shared alongside session recordings and follow-up communications.

3.7 How will ELTO share updates to documents and design decisions?

ELTO will provide regular updates through:

- documentation releases;
- developer portal updates;
- webinars and drop in sessions;
- direct communication to nominated contacts.

3.8 Can insurers nominate additional attendees for future webinars?

Yes. Insurers can nominate additional colleagues for future webinars and engagement sessions.

This may include colleagues from policy operations, delegated authority teams, IT, data, compliance, testing, portal administration and transition planning.

3.9 Can we ask questions on the API documentation once it is released?

Yes. Questions can be raised via ELDNextGen@elto.org.uk
ELTO will also provide technical drop-in sessions to support implementation queries.

3.10 How should insurers raise issues, clarifications or risks?

All ELD NextGen queries, including technical, business and transition-related questions, should be sent to ELDNextGen@elto.org.uk

This is the primary contact route for the programme.

Any issues accessing the ELD Portal or Developer Portal should be raised with Helpdesk and sent to Elto.ISHelpdesk@elto.org.uk

Any future changes to contact routes will be communicated as part of the transition and cutover plan.

3.11 How often will ELTO provide updates?

ELTO will provide regular updates throughout the transition period.

These will include:

- documentation updates;
- design decisions;
- confirmed API details;
- transition guidance;
- webinar invitations;
- testing guidance;
- cutover communications.

3.12 Are worked examples or screenshots available for API file uploads?

Yes. The Developer Portal shows endpoint request/response examples and the Getting Started guidance includes screenshots of the portal and API areas. The File Transfer Guide also explains the API-led SAS upload flow. Developers should use the Developer Portal for the current endpoint examples.

3.13 Will insurers still have a KAU or named relationship contact?

Future engagement and relationship management arrangements will be confirmed as part of the transition and cutover plan.

Existing relationship and support routes should continue to be used until any changes are confirmed.

4 Portal Access, Registration & User Administration

Questions in this section

4.1 Will existing portal usernames and passwords remain the same? 11

4.2 Will users need multiple email addresses if they act for more than one organisation? 11

4.3 How will users be verified and secured in the new portal? 12

4.4 Will one-time verification codes continue? 12

4.5 Will password expiry or reset frequency change? 12

4.6 How many onboarding contacts should each insurer nominate? 12

4.7 What are API credentials? 12

4.8 Does the API use an API key? 12

4.9 Will API Credentials expire automatically? 13

4.10 How long does a bearer token last? 13

4.11 Are API credentials the same as portal usernames and passwords? 13

4.12 What domains need to be whitelisted to enable me to access the APIs? 13

4.13 Will the portal support manual policy management? 13

4.14 Will the portal support bulk file upload? 13

4.15 How will access work where an organisation acts as both an insurer and a delegated authority? 14

4.1 Will existing portal usernames and passwords remain the same?

No. There will be no migration of existing usernames and passwords from the current platform to the new platform.

All users will need to register for the new platform.

4.2 Will users need multiple email addresses if they act for more than one organisation?

No. In the new platform, a single user account will be able to access multiple suppliers or organisations, subject to the correct permissions.

Users do not need separate email addresses simply to access multiple organisations.

4.3 How will users be verified and secured in the new portal?

Access is provisioned to the email address supplied during onboarding. Where the organisation has Microsoft Entra, the user signs in with the organisational credentials associated with that email address and completes MFA. Where the organisation does not have an Entra tenant, a one-time passcode is sent to the user's email address and uses SMS as part of MFA.

4.4 Will one-time verification codes continue?

One-time passcodes will be supported where required.

Further detail will be included in the transition and cutover plan.

4.5 Will password expiry or reset frequency change?

For the ELD portal, authentication follows the Microsoft Entra / one-time-passcode flow described in the Getting Started Guide and does not require a password. The Developer Portal uses a separate sign-in service and provides its own password-reset function.

4.6 How many onboarding contacts should each insurer nominate?

ELTO will ask each insurer to nominate appropriate operational and technical contacts for onboarding.
Each insurer should nominate:

- 1 lead contact;
- 1–2 technical or integration contacts;
- up to 5 developer users for developer portal access.

These limits are intended to support onboarding and may be reviewed as the programme progresses.

4.7 What are API credentials?

API credentials are application credentials used to authenticate system-to-system requests. A Test or Production credential is created in the ELD portal using the public certificate from a certificate key pair. The corresponding private key stays under the organisation's secure control and is used to obtain a short-lived bearer token from Microsoft Entra ID. The bearer token is then sent with API calls.

4.8 Does the API use an API key?

No. The API uses certificate-backed credentials and a bearer token rather than a shared API key. The token is included in the Authorization header of each request.

4.9 Will API Credentials expire automatically?

Yes. A credential can be valid for no more than 365 days. If the certificate has a shorter validity period, the credential reflects that shorter period; a longer period is capped at 365 days. Organisations should plan renewal before expiry and remove credentials no longer required.

4.10 How long does a bearer token last?

Bearer tokens last for 60 minutes. Integrations should obtain tokens programmatically and must not reuse an expired token. Test credentials and tokens cannot be used against Production endpoints.

4.11 Are API credentials the same as portal usernames and passwords?

No. Portal usernames and access are used by individual users to log into the ELD portal. API credentials are used by systems or applications to submit data through the API.

4.12 What domains need to be whitelisted to enable me to access the APIs?

The following domain and subdomains are required for access to the APIs:

- developer.eltohub.org.uk
- mgmt.eltohub.org.uk
- eltohub.org.uk
- api.eltohub.org.uk
- f3485bd8-28c0-4a51-b6d1-806029a15230.ciamlogin.com/

4.13 Will the portal support manual policy management?

Yes. The portal will support manual single policy management.

This includes:

- creating a single policy;
- updating a single policy;
- deleting a single policy;
- checking submission status;
- reviewing validation results.

4.14 Will the portal support bulk file upload?

No. Bulk file upload will be available through the API only.

The portal will support manual single policy submission and status checking, but not bulk policy file upload through the user interface.

4.15 How will access work where an organisation acts as both an insurer and a delegated authority?

The new platform is intended to support a more flexible access model.

A single user will be able to access multiple organisations where they have the correct permissions. Detailed guidance on how access is configured and managed will be included in the transition and cutover plan.

5 Policy Data Model & Policy Key

Question in this section

5.1 What is the new policy key? 15

5.2 Is the policy key the same as the compend or composite key? 16

5.3 What happens if the policyholder name changes? 16

5.4 Should we change how we populate the Supplementary Policy Reference, previously the DA/Broker Ref? 16

5.5 What happens if an employer name changes? 16

5.6 What happens if the cover end date changes because of a mid-term cancellation? 17

5.7 Will Original Insurer name or Original Insurer ID still be referenced? 17

5.8 Will the removal of Original Insurer ID affect policy tracing work? 17

5.9 How will annual reconciliation work if the policy key is changing? 17

5.10 What is the difference between PolicyholderName and Employer name? 17

5.11 Where should subsidiary companies be supplied? 17

5.12 What is InsurerRef and does it replace SiteId? 17

5.13 Is Transaction Type still required? 17

5.14 What date format must be used? 18

5.15 How should master-policy, binder or delegated-arrangement references be represented? 18

5.16 Does the new model support multiple ERNs for one employer? 18

5.17 Will additional ERNs be migrated automatically? 18

5.18 What is a CRN? 18

5.19 Will leaving CRN blank create an audit issue? 18

5.20 Is CRN mandatory? 18

5.1 What is the new policy key?

The new policy key is derived by the following fields:

- Insurer ID;
- policy number;
- Policyholder name;

- supplementary policy reference;
- cover start date;

5.2 Is the policy key the same as the compend or composite key?

Yes - “policy key” is the NextGen term for the combination used to uniquely identify a policy record.

5.3 What happens if the policyholder name changes?

Policyholder name is part of the policy key. Where a policyholder name changes then a new policy will be created.

5.4 Should we change how we populate the Supplementary Policy Reference, previously the DA/Broker Ref?

No. Insurers and delegated authorities should continue to populate the Supplementary Policy Reference using the same convention they use today.

The Supplementary Policy Reference forms part of the ELD policy key. This means that changing the value, including removing or changing characters such as a full stop (.), hyphen (-) or another character, may cause the ELD to identify the submission as a different policy rather than an update to the existing policy.

For example, where an organisation currently uses a full stop, hyphen or another character when the DA/Broker Ref would otherwise be blank, it should continue to submit the same value in the Supplementary Policy Reference in the NextGen ELD.

Similarly, where the field is genuinely left blank today, organisations should continue with their existing approach.

Organisations should therefore not clean, standardise or change existing Supplementary Policy Reference values as part of the transition to NextGen ELD, unless specifically instructed by ELTO. Maintaining the existing value will help ensure that subsequent submissions continue to match the correct policy record.

5.5 What happens if an employer name changes?

Employer name is not part of the policy key.

The effect of an employer name change will depend on how the policy record is submitted. As policies must be submitted in full, the submission must include the complete and correct list of employers for that policy.

5.6 What happens if the cover end date changes because of a mid-term cancellation?

Cover end date is no longer part of the policy key. A revised cover end date is treated as an update to the full policy record, not a change to the policy key. ELTO will provide worked examples for mid-term cancellations in the API guidance.

5.7 Will Original Insurer name or Original Insurer ID still be referenced?

OriginalInsurerId is not submitted in the new API. However, originalInsurerName is a required field in the current Policy Input schema. It should identify the insurer that originally underwrote the policy. The Schema Guide states that if the historic original insurer is unknown, use “Not Known”.

5.8 Will the removal of Original Insurer ID affect policy tracing work?

The removal of the original insurer ID should not affect tracing. Policy history will be maintained and kept within the audit logs internally. Further guidance on tracing will be provided if required.

5.9 How will annual reconciliation work if the policy key is changing?

Guidance on reconciliation processes will be included in the transition and cutover plan.

5.10 What is the difference between PolicyholderName and Employer name?

Policyholder Name is the name of the main policyholder associated with the policy. Employers Name identifies each employer covered for Employers’ Liability under that policy. A policy contains one or more employers.

5.11 Where should subsidiary companies be supplied?

Where a subsidiary is an employer covered by the policy, it should be included as an item in the employers array. The NextGen model removes the legacy parent/child hierarchy and represents all covered employers within the single policy record.

5.12 What is InsurerRef and does it replace SiteId?

InsurerRef is an optional insurer-defined reference that can be used to associate the ELD record with an internal source system, product or other reference. SiteId is not part of the new ingestion schema. The insurer is identified in the API path and validated against the authenticated credential; supplier context is derived from authentication.

5.13 Is Transaction Type still required?

No. Transaction Type is not part of the current PolicyInput or file-transfer schema and is no longer needing to be supplied. The operations is determined by the API being called.

5.14 What date format must be used?

Policy and adjusted cover dates use ISO 8601 date format: YYYY-MM-DD, for example 2026-01-01.

5.15 How should master-policy, binder or delegated-arrangement references be represented?

Where a master policy, binder or delegated arrangement results in the same Policy Number being used across multiple records, the Supplementary Policy Reference should be used to distinguish the individual policy records.

The ELD policy key is made up of: Insurer ID + Policy Number + Policyholder Name + Supplementary Policy Reference + Cover Start Date

This combination ensures each policy record can be uniquely identified.

Where the same Policy Number is used across a delegated arrangement or broker scheme, the Supplementary Policy Reference should therefore be used to identify the individual record. If the Supplementary Policy Reference is also the same, the combination of Policyholder Name and Cover Start Date will provide the remaining distinction within the policy key.

5.16 Does the new model support multiple ERNs for one employer?

Yes. ERNs are now held as an array, allowing multiple Employer Reference Numbers to be supplied for a single employer.

5.17 Will additional ERNs be migrated automatically?

The ERN currently held on ELD will be carried over where one exists.

Additional ERNs held by insurers can be submitted after migration as part of standard policy submissions.

5.18 What is a CRN?

CRN means Company Registration Number. It is the unique company registration reference issued by Companies House. CRN is optional in the new ELD model and may be left blank where the insurer does not hold it.

5.19 Will leaving CRN blank create an audit issue?

CRN is optional. Leaving it blank will not result in a validation failure where the value is not held.

Further audit guidance will be provided if required.

5.20 Is CRN mandatory?

No. CRN is optional.

If an insurer does not hold CRN in its source systems, it may be left blank.

6 Parent / Child Policy Changes

Question in this section

6.1 What happens to the existing parent/child employer hierarchy? 20

6.2 Will insurers still supply parent and child records as they do today? 20

6.3 How will the new platform distinguish between what used to be parent and child records? 20

6.4 How will child employer cover periods be handled? 20

6.5 Will a child employer's shorter cover period still be visible? 21

6.6 How will ELTO know that every employer has been supplied? 21

6.7 How will the system avoid overwriting a parent record where the employer is actually a subsidiary? 21

6.8 What happens if there are multiple employers with the same company name but different addresses? 21

6.9 Will subsidiary employers need an address? 21

6.10 What should insurers do if they have high-volume parent/child submissions today? 21

6.1 What happens to the existing parent/child employer hierarchy?

The parent/child structure is removed.

In the new model, each policy is submitted as a single policy record containing all covered employers, with no hierarchy between them.

6.2 Will insurers still supply parent and child records as they do today?

No. Policies must be submitted as a single policy record containing all covered employers.

6.3 How will the new platform distinguish between what used to be parent and child records?

The new platform does not use a parent/child distinction.

All employers are submitted within a single policy record.

6.4 How will child employer cover periods be handled?

Where an employer starts later than the overall policy start or ends earlier than the overall policy end, use adjustedCoverStartDate and/or adjustedCoverEndDate for that employer. The

policy-level coverStartDate and coverEndDate remain required and represent the overall policy period.

6.5 Will a child employer's shorter cover period still be visible?

Yes. Different employer coverage periods are reflected using the adjusted employer cover date fields.

6.6 How will ELTO know that every employer has been supplied?

Each submission for a policy key is treated as a complete policy record.

The submitting organisation must include all employers that should be associated with that policy. Any employer omitted from a submission will be treated as no longer part of the policy.

6.7 How will the system avoid overwriting a parent record where the employer is actually a subsidiary?

The system does not distinguish between parent and subsidiary entities.

Each submission replaces the full policy record, which must include all employers that should remain on the policy.

6.8 What happens if there are multiple employers with the same company name but different addresses?

The new model allows multiple employers to be held within a single policy record, each with its own address and identifiers. The current outline only specifies duplicate policy detection. Additional employer-level duplicate validation rules will be defined in the full API documentation.

6.9 Will subsidiary employers need an address?

Yes. Each employer record should include an address to support accurate policy searching and identification.

For migrated records, where a subsidiary or employer address is currently blank, the Policyholder address will be used for migration purposes.

Going forward, insurers should capture and submit the actual employer address wherever possible, as this will improve search accuracy within the ELD. Where an employer-specific address is not available, the Policyholder address may be submitted instead.

6.10 What should insurers do if they have high-volume parent/child submissions today?

Insurers with high-volume parent/child submissions should raise this during transition planning.

This will be addressed as part of onboarding and testing to support file structure and implementation changes.

7 Submission Routes & File Formats

Question in this section

7.1 What submission routes will be available? 23
7.2 What is direct API submission? 24
7.3 What is API file upload? 24
7.4 What file formats will be supported? 24
7.5 Is the new text file a CSV file? 24
7.6 What happens if a field contains a pipe character? 24
7.7 Will there be maximum field lengths? 25
7.8 Can insurers still submit single policies through the portal? 25
7.9 Can insurers upload bulk files through the portal? 25
7.10 How should smaller batches be submitted if the portal does not support file upload? 25
7.11 Can deletes be submitted by file? 25
7.12 Does a pipe-delimited file require a header row? 25
7.13 What are the current size and record limits? 25
7.14 How does the API file-upload process work? 26
7.15 What fields are in the pipe-delimited text file? 26
7.16 Can the portal be used for single policy deletes? 26
7.17 Will there be a GET API to retrieve ELD policy details? 26
7.18 Can a policy be partially updated? 26

7.1 What submission routes will be available?

There are two API-based submission routes:

1. Direct API submission
   Used for smaller submissions or where immediate validation feedback is required.
2. API file upload
   Used for bulk submissions, scheduled data loads and existing batch processes.

The portal will also support manual single policy submission.

7.2 What is direct API submission?

Direct API submission allows one or more policies to be submitted directly in the API request body.

Validation is synchronous and all-or-nothing. If any policy in the request fails validation, the entire submission is rejected.

7.3 What is API file upload?

API file upload allows an organisation to:

- request a secure upload URL;
- upload a file to that URL;
- track processing using the status endpoint or ELD policy management area.

Processing is asynchronous. Valid policy records are accepted and invalid records are rejected individually.

7.4 What file formats will be supported?

For file-based submissions, the system supports:

- JSON;
- pipe-delimited text.

JSON is recommended for new integrations. Pipe-delimited text supports organisations using spreadsheet or batch-based data formats.

7.5 Is the new text file a CSV file?

No. The text file is pipe-delimited rather than comma-separated.

It may be produced from spreadsheet tools, but it must follow the expected pipe-delimited structure and column order.

7.6 What happens if a field contains a pipe character?

The pipe character is used as the field separator in the text file format.

If a field value itself contains a pipe character, the whole field must be enclosed in double quotes. This prevents the pipe character being treated as a field separator.

For example: Employer name: `Employer | Trading Ltd` should be supplied as: `"Employer | Trading Ltd"`

If a field contains double quotes, each double quote must be doubled.

For example: `Employer "North" Ltd` should be supplied as: `"Employer ""North"" Ltd"`

7.7 Will there be maximum field lengths?

Yes. Field lengths and machine-readable validation constraints are now defined in the published OpenAPI/Developer Portal. Examples include policyNumber and supplementaryPolicyReference max 75 characters, policyholderName max 250, originalInsurerName max 100 and insurerRef max 100. Use the current Developer Portal definition for the complete rule set.

7.8 Can insurers still submit single policies through the portal?

Yes. The portal will support single policy submission, including create/update and delete actions.

The portal will also support status checking and validation result review.

7.9 Can insurers upload bulk files through the portal?

No. Bulk file upload will be available through the API only.

The ELD portal user interface will not support bulk policy file upload.

7.10 How should smaller batches be submitted if the portal does not support file upload?

Smaller batches that are not suitable for manual portal entry should be submitted via the API.

Direct API submission is suitable for smaller or real-time batches. API file upload should be used for larger batches.

Insurers should consider whether direct API submission or API file upload is more appropriate depending on the size and frequency of the batch.

7.11 Can deletes be submitted by file?

Not at present. The file-upload request schema allows operationType=UPSERT only. Direct DELETE is available as a separate endpoint. A future feature enhancement may make this available post launch as part of the ELD roadmap.

7.12 Does a pipe-delimited file require a header row?

Yes. The File Transfer Guide provides full details of the required header row and expected headings. Each data row must keep the same column count as the header, including blank optional fields represented by consecutive pipe delimiters.

7.13 What are the current size and record limits?

Direct policy requests are limited to 2 MB and the current OpenAPI allows 1 to 5,000 policy items per direct UPSERT or DELETE request. There is no set file-size limit and no separately stated file record-count limit, for file uploads. Note however, the SAS upload URL lasts 60 minutes.

7.14 How does the API file-upload process work?

1) POST file metadata to the file-upload endpoint and receive uploadId, uploadUrl and expiresAt.
2) PUT the file to the returned SAS uploadUrl using x-ms-blob-type: BlockBlob and the correct Content-Type.
3) Poll the status endpoint using uploadId no more than once every 30 seconds.
Note: Upload completion does not itself mean policy validation has completed.

7.15 What fields are in the pipe-delimited text file?

The File Transfer Guide defines the complete ordered header and worked examples.

7.16 Can the portal be used for single policy deletes?

Yes. The portal will support manual single policy create, update and delete actions. Bulk file upload will be API only.

7.17 Will there be a GET API to retrieve ELD policy details?

A GET API for retrieving policy details is not included in the current specification. The current scope focuses on submission, file upload, delete and submission status. Any future retrieval capability will be confirmed.

7.18 Can a policy be partially updated?

No. Policies must be submitted in full.

Where a policy with the same policy key already exists, the accepted policy submission replaces the previous version once processing is complete.

8 Validation, Errors and Submission Status

Question in this section

8.1 How does validation work for direct API submissions? 27

8.2 How does validation work for file uploads? 28

8.3 If one employer fails validation, does the rest of the policy still load? 28

8.4 What happens if the file itself is invalid? 28

8.5 How will validation errors be returned? 28

8.6 How will submission status be monitored? 28

8.7 Will insurers receive a return file listing failed transactions? 28

8.8 Will validation errors include enough information to identify the failed record? 29

8.9 What status values will be used? 29

8.10 Does the status endpoint confirm how many policies were actually deleted? 29

8.11 What happens if a DELETE request refers to a policy that does not exist? 29

8.12 What does “accepted and queued” mean? 29

8.13 Where can results be viewed after a file upload? 30

8.14 Can validation results be downloaded from the portal? 30

8.15 Will ELTO share the field-level validations used in the new processing flow? 30

8.16 When a file upload is processed, are errors reported at file level or record level? 30

8.17 When the documentation says valid policies are accepted and invalid ones rejected, does this mean files or records? 30

8.18 What should an integration do after a 429 response? 30

8.19 What is the difference between 401 and 403? 31

8.20 Will load results still be easy to review without an email confirmation? 31

8.21 How will everyday policy scenarios be handled? 31

8.1 How does validation work for direct API submissions?

For direct API submissions, validation is synchronous and all-or-nothing.

If any policy record in the submission fails validation, the entire submission is rejected and no records are accepted or queued.

8.2 How does validation work for file uploads?

For file uploads, validation is asynchronous and processed per policy record.

Valid policy records are accepted and invalid records are rejected individually. There is no minimum pass rate.

8.3 If one employer fails validation, does the rest of the policy still load?

Validation is applied at a policy record level.

For direct API submissions, if any policy record fails validation, the entire submission is rejected.

For file uploads, valid policy records are accepted and invalid policy records are rejected individually.

Within a policy record, validation failures prevent that policy record from being accepted.

8.4 What happens if the file itself is invalid?

If a file cannot be processed, it is rejected in full and no policy records are processed.

Examples include:

- malformed JSON;
- invalid pipe-delimited structure;
- missing or incorrect header row;
- incorrect column count.

8.5 How will validation errors be returned?

For direct API submissions, validation errors are returned immediately in the API response.

For file uploads, validation results are available after processing via:

- the API status endpoint;
- the ELD policy management area.

8.6 How will submission status be monitored?

File-upload status is retrieved using the file upload status endpoint. Poll no more than once every 30 seconds. The ELD portal also provides visibility of submission status and validation results.

8.7 Will insurers receive a return file listing failed transactions?

The system does not produce a separate return file.

For file-based submissions, validation results are retrieved using the status endpoint or viewed in the ELD portal.

Availability of export or download functionality will be confirmed.

8.8 Will validation errors include enough information to identify the failed record?

The status response provides sufficient detail to identify the affected record.

This may include:

- policy key;
- employer name;
- policy index (as part of the path);
- employer index (as part of the path);
- field path;
- error description;
- row number for pipe-delimited text files where applicable.

8.9 What status values will be used?

The status endpoint indicates the processing state of a submission.

Status values include:

- waiting for file;
- queued;
- processing;
- complete;
- rejected;
- system error.

Waiting for file, Queued and Processing are intermediate. Complete, Rejected and System Error are terminal and polling should stop.

8.10 Does the status endpoint confirm how many policies were actually deleted?

For DELETE submissions, the status response confirms whether delete records were valid for processing. It does not confirm how many existing policies were deleted. Insurers should validate this through reporting or policy search.

8.11 What happens if a DELETE request refers to a policy that does not exist?

This will be confirmed in API documentation. If the request is validly structured, it will be processed according to standard validation and status rules. See also question 8.10.

8.12 What does “accepted and queued” mean?

The meaning depends on the route. For the direct UPSERT/DELETE endpoints, 200 means the request passed Test validation and has been accepted. For file uploads, the upload/status

lifecycle is asynchronous: receiving/uploading the file is not the same as validation completion, so use the status endpoint until a terminal state is reached.

8.13 Where can results be viewed after a file upload?

Results can be accessed by:

- Querying the API status endpoint using the upload ID;
- viewing submission status and validation results in the ELD policy management area.

8.14 Can validation results be downloaded from the portal?

Validation results are available via the status endpoint and ELD policy management area.

Availability of downloaded of exportable results will be confirmed.

8.15 Will ELTO share the field-level validations used in the new processing flow?

Yes. The Developer Portal OpenAPI now publishes machine-readable field constraints and endpoint request schemas. The Policy Schema Guide explains field purpose. Use the current Developer Portal for all latest definitions.

8.16 When a file upload is processed, are errors reported at file level or record level?

Both can occur. If the file structure is invalid, for example malformed JSON or an invalid pipe-delimited structure, the file is rejected in full.

If the file is structurally valid, validation is applied per policy record:

- valid policy records are accepted;
- invalid policy records are rejected individually.

8.17 When the documentation says valid policies are accepted and invalid ones rejected, does this mean files or records?

For file uploads, validation operates at policy record level.

Once the file is accepted for processing:

- valid policy records are processed;
- invalid policy records are rejected individually.

8.18 What should an integration do after a 429 response?

Wait for the number of seconds specified in the Retry-After response header before retrying. Do not retry in a tight loop. The current Getting Started guidance states API throttling of 60 requests per minute and 5,000 requests per day.

8.19 What is the difference between 401 and 403?

401 means the request is not authenticated, for example because the bearer token is missing, invalid or expired. 403 means the token is valid but the credential is not authorised for the insurerId in the request path.

8.20 Will load results still be easy to review without an email confirmation?

Yes. File-processing status, valid/rejected policy counts and validation errors are available through the status endpoint and through the ELD policy management area.

8.21 How will everyday policy scenarios be handled?

The following are common scenarios and expected handling.

Scenario	What happens
Policyholder name correction	If the policy key stays the same, the corrected name updates the existing policy record.
Mid-term cancellation	As cover end date is not part of the policy key, a revised cover date is treated as an update to the full policy record.
Adding / removing an employer	Re-submit the full policy record with the complete employer list. The new version replaces the previous one. If adding an employer later or removing one earlier, but they still have a period of cover then the adjusted cover dates should be updated.
File upload with validation failures	For file uploads, valid policies are accepted and invalid policies are rejected individually. Errors are viewed via the status endpoint or ELD portal.

9 Testing, Reporting and Ongoing Operations

Question in this section

9.1 Will test endpoints be available? 32

9.2 When will test endpoints be available? 33

9.3 Which test endpoints will be available first? 33

9.4 What testing of the APIs will members be expected to complete? 33

9.5 Will ELTO issue testing scenarios to support cut-over readiness? 33

9.6 Will there be a UAT sign-off date? 33

9.7 Will insurers be able to run their own reports? 33

9.8 Will website search functionality for policyholders change? 33

9.9 Will the changes affect how ELTO makes regular policy tracing requests to members? 33

9.10 What hypercare support will ELTO provide after go-live? 34

9.11 How will ELTO support members during the January–March period, given audit and regulatory activity? 34

9.12 Will policy tracing requests be affected by these changes? 34

9.13 Will insurers be able to run reports to validate changes? 34

9.14 What happens to data sent to the Test API? 34

9.15 How can we identify the source of a policy submission now that SiteId is removed? 34

9.16 Will the weekly tracing-file structure change? 34

9.17 Will other FTP-based downloads be affected? 35

9.18 What architecture, security and logging standards should insurer integrations follow? 35

9.19 Is there a specification for the annual audit file? 35

9.20 What should insurers do now? 36

9.1 Will test endpoints be available?

Yes. The Test API is available. It provides authenticated health, direct UPSERT validation, direct DELETE validation, file-upload initiation and file-upload status operations. Direct Test UPSERT/DELETE do not persist policy data.

9.2 When will test endpoints be available?

The Test API endpoints and Developer Portal documentation are available now for insurer development and integration testing. Insurers should use the live Developer Portal to confirm the current endpoint set and version.

9.3 Which test endpoints will be available first?

The current published Test API includes: GET health; POST direct policies upload; DELETE direct policies; POST request policy file upload; and GET policy file upload status.

9.4 What testing of the APIs will members be expected to complete?

The Getting Started Guide provides a recommended, non-prescriptive test approach covering connectivity/authentication, valid direct UPSERT, direct DELETE, file flow, invalid/mixed files, representative volume/retry behaviour, credential replacement and operational readiness. Insurers should tailor testing to their architecture and risk.

9.5 Will ELTO issue testing scenarios to support cut-over readiness?

The Getting Started Guide provides recommended checks and edge cases for insurer testing. These are a practical starting point rather than a mandatory script.

9.6 Will there be a UAT sign-off date?

The UAT sign-off will be managed by ELTO. Insurers will not have access to a UAT environment, only the test endpoints that have been provided. The testing approach and assurance will be provided transition and cutover plan.

9.7 Will insurers be able to run their own reports?

Reporting capability will be defined in future guidance.

The platform will provide improved visibility of submissions, status and validation outcomes.

9.8 Will website search functionality for policyholders change?

Changes to policyholder-facing search functionality will be confirmed.

This includes any enhancements to search capability or matching logic.

9.9 Will the changes affect how ELTO makes regular policy tracing requests to members?

This is not expected to be the main focus of the policy submission change.

ELTO will confirm whether any operational changes will affect policy tracing requests or member responses.

9.10 What hypercare support will ELTO provide after go-live?

Post-go-live support will be provided as part of the transition.

Details of the hypercare period, support channels and escalation routes will be defined in the transition and cutover plan.

9.11 How will ELTO support members during the January–March period, given audit and regulatory activity?

ELTO recognises that January to March is a peak period for audit and regulatory activity.

The transition and cutover plan will define timing, testing expectations and support arrangements to enable insurers to plan accordingly.

Any specific risks should be raised as early as possible.

9.12 Will policy tracing requests be affected by these changes?

No. Existing tracing cases will be migrated to the new platform.

Further detail will be included in the transition and cutover plan.

9.13 Will insurers be able to run reports to validate changes?

Reporting guidance will define how insurers can validate submitted data and changes.

9.14 What happens to data sent to the Test API?

Direct Test UPSERT and DELETE requests are validated but the policy data is not written into the ELD. Test files are temporarily stored in the Test environment so asynchronous validation/status reporting can run; Test processing records and validation results are retained for 8 weeks and do not progress to the ELD policy layer.

9.15 How can we identify the source of a policy submission now that SiteId is removed?

The insurer is selected through insurerId and authenticated credentials provide supplier context. The insurer can also populate the optional insurerRef field with an internal source-system, product or other reference.

9.16 Will the weekly tracing-file structure change?

The tracing file will be sent via CSV only and continue to be issued as an attachment. The file will remain as close to the current format as possible, however, as the schema has changed it is anticipated there will be minor changes to the file. A confirmed specification and sample will be issued in the November.

9.17 Will other FTP-based downloads be affected?

Yes. As part of the ELD NextGen transition, ELD services will move to API-based delivery and the legacy SFTP service will be decommissioned.

Any third-party integrations, automated processes or scheduled jobs that currently rely on FTP/SFTP will therefore need to be reviewed and updated to work with the new platform services and data structures.

Insurers should identify any existing automated FTP/SFTP processes as part of their transition planning and allow time to amend and test these before cutover.

9.18 What architecture, security and logging standards should insurer integrations follow?

ELTO does not prescribe a specific internal architecture or technology stack for insurer integrations. Each insurer should design and operate its integration in line with its own security, architecture and change-management standards.

As a minimum, integrations should support the published ELD authentication and API requirements and have appropriate controls in place for:

- secure storage and management of certificates, private keys and credentials;
- separation of test and production environments and credentials;
- controlled access to integration components and secrets;
- logging of API requests, responses, timestamps, status codes and correlation/request identifiers;
- monitoring and alerting for failed submissions, authentication failures and repeated processing errors;
- appropriate retry and recovery handling; and
- sufficient audit information to support investigation and operational support.

Sensitive information such as private keys, bearer tokens and other credentials should not be written to logs or support evidence.

Insurers should apply their own organisational security, regulatory and operational policies alongside the technical requirements published by ELTO.

9.19 Is there a specification for the annual audit file?

For transition to ELD NextGen, ELTO will provide insurers with a full extract of their policy data, in line with the current annual audit output, together with a snapshot report within the ELD Portal showing the data held at the point of go-live.

Following launch, insurers will continue to be able to access the All Policies report through the ELD Portal.

A more detailed specification for the audit/reporting output will be provided ahead of launch, with the current intention to publish this by January 2027.

9.20 What should insurers do now?

Insurers should:

- review the ELD NextGen documentation;
- identify current SFTP feeds and batch processes;
- determine preferred submission routes;
- confirm ownership of API integration;
- identify portal users;
- nominate technical and operational contacts;
- review delegated authority arrangements;
- prepare for onboarding and testing;
- raise any transition risks as early as possible via ELDNextGen@elto.org.uk