Home Office

Passport cancellations: malicious lost and stolen reports

Version 13.0

This guidance tells His Majesty's Passport Office staff how to deal with malicious lost and stolen passport reports.

Contents

About, Passport cancellations: malicious lost and stolen reports

This guidance tells His Majesty's Passport Office staff how to deal with customer queries, when a malicious lost and stolen report has resulted in the cancellation of a passport (from a loss report).

Contacts

If you have any questions about the guidance and your line manager or senior caseworker cannot help you or you think that the guidance has factual errors then email the Guidance team.

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email the Guidance team.

Publication

Below is information on when this version of the guidance was published:

- version **13.0**
- published for Home Office staff on **22 October 2025**

Changes from last version of this guidance

This guidance has been updated in the section Examiner decides LS report was made maliciously, to change references from Child Protection and Safeguarding team (CPST) to Public Protection Specialist Safeguarding team (PP SST), following a team name change.

Related content
Contents

Malicious lost and stolen reports

This section tells HM Passport Office staff, what a lost and stolen report is and includes what malicious lost and stolen reports are, how we might receive one and how to deal with it.

When a customer declares their passport as lost or stolen, HM Passport Office will electronically cancel it in our records.

A customer can make us aware of a lost or stolen passport by:

- completing a paper LS01 form
- using a Digital Lost and Stolen (DLSR) report from GOV.UK
- phone using our Adviceline

HM Passport Office can also receive notification of a lost or stolen passport from trusted sources, such as the Foreign Commonwealth and Development Office (FCDO).

International third party and child reports are processed by the central LSR team.

Examination staff can create and cancel a lost or stolen report on behalf of the customer in line with guidance, if they find out a passport has been:

- lost or stolen and the customer has not already made a report
- reported lost or stolen in error

When a customer reports their passport lost or stolen online, the DLSR team will receive and deal with the report.

If the customer makes a lost or stolen report by completing a paper LS01 form or by phone, the Lost Stolen or Recovered (LSR) team will deal with the report.

The LSR team will also deal with any complex cases referred to them by the DLSR team.

What a malicious report is

A person may falsely, fraudulently or dishonestly declare another person's passport as lost or stolen for malicious reasons. These include but are not limited to:

- stopping a person from traveling
- inconveniencing a person
- causing them harm
- parental or child disputes

If the person provides all of the information we need to process an LSR report on:

- an adult passport, we will:
  - cancel the passport and record it as ‘lost’ or ‘stolen’ on our passport records
  - not carry out further checks
- a child passport, we will:
  - confirm that the person reporting the cancellation is the person who originally applied for the child passport
  - carry out further checks before deciding if the passport should be cancelled (in line with the LSR examiner guidance)

If a third party made the LSR report maliciously, the passport holder may not be aware.

How malicious LS reports are identified

The passport holder may find out that their passport has been electronically cancelled and a lost and stolen (LS) record created when they:

- are using the passport for travel (during Border Force, or overseas immigration checks when the customer tries to leave or enter the UK)
- are using the passport for identity checks (if the check includes passport validation, and a data verification (DVA) check)
- receive a DLSR notification by text or email
- receive a phone call from the LSR or DLSR team
- are speaking to:
  - the person who submitted the malicious report
  - a third party who is aware of the malicious report

HM Passport Office may become aware of a malicious report when the customer:

- contacts us (by phone, email, or by attending a passport office) asking why:
  - their passport is cancelled (for example, if Border Force have told the customer their passport has been cancelled)
  - they have received a DLSR notification
  - we have issued a new passport, when they still have a current valid passport
- tells us they did not submit a loss declaration, when:
  - Digital Lost Stolen Reporting (DLSR) team contacts them about a DLSR report they are processing
  - the central LSR team contact them
  - an examiner contacts them if they are processing an application
- provides a covering letter to state their new application is to replace a passport that was previously cancelled by someone else

Related content
Contents

Examiners dealing with malicious LS reports

This section tells HM Passport Office examiners how to deal with passport applications when customers tell us about a malicious passport cancellation report.

A customer can make us aware of a malicious report, when you (the examiner) are dealing with an application for them. For example, the customer may:

- provide a covering letter with their application to tell you they did not cancel their previous passport
- tell you the previous passport was reported lost or stolen by someone else, when you contact them in relation to their application

If the customer makes you aware of a malicious lost or stolen (LS) report when dealing with their application, you must:

1. Search lost and stolen records (LSR) using the customer's details to find the loss report.
2. Associate the LS report to the application, by selecting **Associate with this application**.
3. Check the reason for cancellation, and who reported the loss.
4. Check to see if any further passports have been issued.

Then, you must decide if the LS report was:

- made maliciously or using false, dishonest, or fraudulent information
- not malicious, for example:
  - HM Passport Office cancelled the passport in error
  - the customer did report the loss but they had forgotten
  - the customer had travelled using the wrong passport (previously reported as lost)

Examiner decides LS report was made maliciously

Where you have decided the previous passport has been cancelled due to a malicious LS report, you must ask the customer if they would like their replacement passport issued as a:

- restricted validity passport:
  - valid until the expiry date on their original cancelled passport; and,
  - issued free of charge (gratis) and we will refund any fee paid for the current application, see Gratis passport applications guidance
- a full validity passport, which they must pay for in full

If the customer has asked for their new passport to be issued with the remaining validity from their cancelled passport, you must ask them to send us either:

- the original cancelled passport; or,
- a receipt or letter to confirm the passport has been retained (for example, by Border Force)

You must follow the Passport fees guidance, to arrange the refund for the customer (if they have asked for their replacement passport to be issued with the remaining validity from their cancelled passport).

You must not continue to process the application, if you have any safeguarding concerns (for example, a child application where there are signs of a parental dispute). You must refer the application to the Triage team, who will liaise with Public Protection Specialist Safeguarding team (PP SST).

Where there are no safeguarding or fraud concerns, you must:

1. Add a case note to the application, to:
   - record the evidence you have received; and,
   - confirm the malicious report
2. Continue to process the application in line with the relevant guidance.

Examiner decides LS report was not malicious

If you decide the report was not malicious, you must tell the customer we:

- have investigated the report
- are satisfied there are no concerns or discrepancies
- will not be taking any further action

You must then continue to process the application in line with the relevant guidance.

If a customer wants to make a complaint

If customer wants to make a complaint you must follow the complaints procedure guidance.

Related content
Contents

CSMT: dealing with malicious LS reports

This section tells HM Passport Office Customer Service Management team how to deal with customers who ask why we have cancelled their passport or tell us they, have not reported the passport lost or believe someone has maliciously cancelled their passport.

You, the Customer Service Management team (CSMT) staff member, can get potential malicious reports from:

- the customer, by phone or email
- staff in an Application Processing Centre (APC), for example, if the customer visits a passport office asking why their passport has been cancelled
- staff on the:
  - Digital Lost Stolen Reporting (DLSR) team
  - Lost, Stolen and Recovered (LSR) team
  - Disclosure team
- the Foreign, Commonwealth & Development Office (FCDO), where a customer is overseas

The customer may:

- know or believe the loss was reported maliciously
- have reported the malicious report and false declaration to the police
- have received a ‘non-disclosure’ letter from the Disclosures team
- not be aware why their passport has been cancelled
- be aware of a dispute between the parents of a child, leading to a passport being cancelled maliciously

You must investigate the customer’s query and the LSR report to decide if the report is malicious. The report may be malicious if, for example, the customer states that they have not cancelled the passport.

Where a malicious report has been identified, a replacement passport will be issued to the customer free of charge (gratis). This passport must be valid until the expiry date of the cancelled passport.

If the customer is overseas and a malicious report has been identified, you must tell them to:

1. Contact the FCDO.
2. Request an Emergency Travel Document (ETD) if they need to travel urgently.
3. Continue to investigate the malicious report in line with this guidance.

CSMT: customer has told us about a malicious report

If you, the CSMT staff member are made aware of a malicious lost or stolen (LS) report, you must:

1. Ask the customer for their details, including their:
   - full name
   - date of birth
   - place of birth
   - contact telephone number
   - contact address
   - email address
   - passport number
2. Check the passport application records for the customer's passport.
3. Search lost and stolen records (LSR) using the customer's details to find the loss report.
4. Check the reason for cancellation, and who reported the loss.
5. Check to see if any further passports have been issued.
6. Decide if the LS report was:
   - made maliciously or using false, dishonest or fraudulent information
   - not malicious, for example HM Passport Office cancelled the passport in error or
   - the customer did report the loss, but they had forgotten

CSMT decides the LS report was made maliciously

If you decide the previous passport has been cancelled due to a malicious LS report, you must contact the customer and ask them if they:

- have an urgent date of travel; and,
- would like their replacement passport issuing as a:
  - gratis passport, with the remaining validity from their original cancelled passport
  - a full validity passport

You must ask the customer to provide evidence if they have an urgent date of travel and provide them with a magic link, so they can apply for an urgent counter application. See Gratis passport applications guidance.

If the customer has not got an urgent date of travel, you must ask them to send us either:

- their previous cancelled passport; or,
- evidence their previous cancelled passport has been retained (for example, if this was retained by Border Force)

You must follow the Gratis passport guidance to arrange for a magic link to be sent to the customer, so they can apply for a standard replacement application.

CSMT decides the LS report was not malicious

If you decide the report was not malicious, you must tell the customer we:

- have investigated the report
- are satisfied there are no concerns or discrepancies
- will not be taking any further action

The customer must apply for a replacement passport through the standard application process and pay the relevant fee.

CSMT: customer has applied using gratis magic link

The customer will receive a gratis replacement passport if:

- you have confirmed the LS report was made maliciously; and,
- the customer has asked for their replacement passport to be issued with the remaining validity of their cancelled passport; and,
- the customer has applied using the magic link provided

You must add a case note to the application to tell the examiner if the new passport must be issued either:

- from the issue date of the original cancelled passport (with the remaining validity)
- with full validity

DAP (Digital Application Processing) will then send the application to the appropriate examination queue, depending on whether the customer has applied using the standard or counter service.

You must then:

7. Send an email to the customer, providing advice to prevent future incidents of malicious reports.
8. Add the details of the malicious report to the CSMT malicious reports log, including the issue date of the replacement passport.
9. Notify the Safeguarding caveats team by email, if the malicious report relates to a child or vulnerable adult's passport.

When the replacement passport has been issued to the customer, you must add a passport note to the customer's replacement passport, to record the customer has previously had a passport cancelled due to a malicious report.

Passport cancelled by HM Passport Office in error

If the passport has been cancelled by HM Passport Office in error, you must issue the customer with a replacement passport free of charge (gratis). This passport must be valid until the expiry date of the cancelled passport.

To issue the replacement passport, you must follow the:

- Gratis passports guidance
- Restricted validity passports guidance

Related content
Contents

How the Disclosure team deal with malicious LS reports

This section tells HM Passport Office Disclosure team staff how to deal with a customer telling us about a malicious lost and stolen (LS) report.

The Disclosure team may find out about potential malicious lost and stolen (LS) reports from the customer, if they send a subject access request (SAR).

The Disclosure team must deal with any formal SARs or other enquiries in line with disclosures guidance.

Checking watchlist matches with Counter Fraud teams

If you find a watchlist match in the customer's details, you must email the Watchlist Management team (WLMT), copying in the Customer Service Management team (CSMT) mailbox.

In the email, you must:

- send the passport holder's details, including:
  - full name
  - date of birth
  - place of birth
  - contact telephone number
  - contact address
  - email address
  - passport number
  - details of the malicious report
- tell WLMT:
  - that you are dealing with a subject access request for information about the passport holder's passport and loss record
  - where the request has come from

The WLMT will reply and tell you if you can disclose the details on the Lost or Stolen (LS) record to the customer.

When you must not disclose to the customer

You must not disclose the loss report details to the customer, when:

- you have identified a malicious report of loss
- WLMT tell you

You must send:

1. The customer a non-disclosure letter telling them the options available.
2. An email, containing the details of the malicious LSR report to the CSMT mailbox.

Related content
Contents

How the LSR team deal with malicious LS reports

This section tells HM Passport Office Lost, Stolen and Recovered team staff how to deal with malicious reports.

The Lost, Stolen and Recovered (LSR) team deal with queries from customers about:

- lost or stolen reports (LS)
- Digital Lost or Stolen Reports (DLSR).

This contact can be:

- from the customer, by phone or email
- on a paper LS01 form
- on a digital lost and stolen report (DLSR) from GOV.UK
- from staff in an Application Processing Centre (APC), for example, if the customer visits a passport office asking why their passport is recorded as lost

The LSR team will also get referrals from the Digital Lost Stolen Reporting team (DLSR), when they process a Digital Lost and Stolen (DLSR) report.

LSR: when the customer has not reported their passport missing

When you, the LSR team member, are contacted by a customer to tell you that they have not submitted the LS or DLSR report, you must:

1. Check the customer's details, including:
    - full name
    - date of birth
    - place of birth
    - contact telephone number
    - contact address
    - email address
    - passport number
    - details of the malicious report
2. Ask the customer to confirm they did not send us the lost or stolen report.
3. Check if the passport is cancelled on the passport records.
4. Add a LS note stating, 'customer advises that they did not cancel their passport, possible malicious report'.

Where the malicious report relates to a child passport, you must complete a watchlist check on the child's identity.

If the passport has been cancelled

If the passport has been cancelled, you must:

1. Tell the customer we will:
   - investigate
   - contact them within 10 working days
2. Send an email to the Customer Service Management team (CSMT) mailbox with the details of the malicious report.
3. Add a LS note stating, "customer advises that they did not cancel their passport, possible malicious report. Please contact the customer."

The CSMT will follow their guidance to investigate and contact the customer to provide an update.

If the passport has not been cancelled

If the passport has not been cancelled, you must:

1. Tell the customer we have not cancelled the passport.
2. Send an email to the CSMT mailbox with the details of the malicious report to be logged.
3. Add a LS note stating, 'malicious cancellation attempt'.
4. Fail the LS record.

If the customer requests any further information about the malicious report, you must advise the customer to submit a complaint or a subject access request (SAR).

Related content
Contents