Whistleblowing – Inbox and SharePoint Process

RECEIVING WHISTLEBLOWER REPORT

Whistleblowing correspondence received in the post.

- Scanning/Post room will identify any postal correspondence from whistleblowers.

- Correspondence delivered to delegated officers to deal with.

Whistleblower report online form

- Completed online whistleblowing forms are auto directed to [redacted] email address.

Whistleblower report taken by phone

- Case officer completes online form available at www.ico.org.uk/whistleblower following the Whistleblowing Process for Advice Staff. *Particular care should be taken to verify whistleblower's email address.* When completing a form on behalf of a customer, case officers must tick the 'I am acting on someone else's behalf box', adding their own details in the About you box and the WB's details (if provided) in the relevant fields.

- Submitted forms will automatically direct to the WB team inbox.

- Delegated officers will create WB case.

Whistleblower report picked up on ICE

<u>ICOCasework Sift</u>

- If an email is identified as being from a whistleblower in the 'icocasework' sift queue on the ICE case management system, the person processing that queue will download a copy of the correspondence and send it to the [redacted] @ico.org.uk inbox.

- The person processing the 'icocasework' queue will then delete the email from their sent items and contact ICEhelp to have the original email deleted from ICE and the icocasework inbox.

- Delegated officers will create a case in the restricted area.

- *NOTE - If delegated officer finds an email has been added to the* [redacted] *@ico.org.uk inbox that does not need to processed under the whistleblowing procedures please forward the email to* *icocasework@ico.org.uk. When forwarding the email please advise how the case should be dealt with in the body of the email eg set up as advice case.*

DP, Public Advice or Business Advice Sift Queues

- If an item is identified in the DP, Public Advice or Business Advice sift queues in ICE it should be allocated to one of the delegated officers (check whistleblowing rota).

- Delegated officer will create a case in the restricted area of SharePoint, download the documents from ICE, add them to the restricted case and contact ICEhelp to have the sift item deleted from ICE and the icocasework inbox.

ICE cases

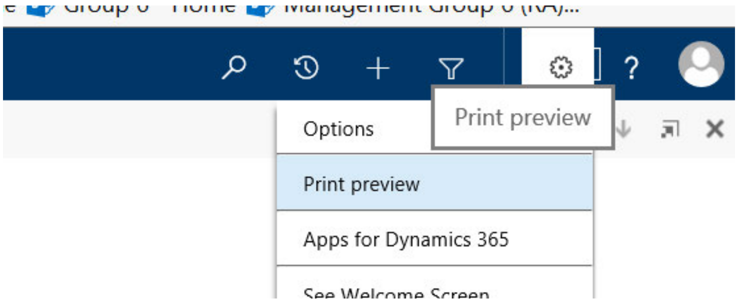
- Whistleblowing cases should not be dealt with on ICE *unless* the individual has also raised concerns about their own personal data. If a whistleblowing item has been missed at sift and a case created in error the case should be allocated to the delegated officer (check whistleblowing rota).

- Delegated officer will create a case in the restricted area of SharePoint, download the documents from ICE, add them to the restricted case and contact ICEhelp to have the ICE case deleted from ICE and correspondence deleted from the icocasework inbox.

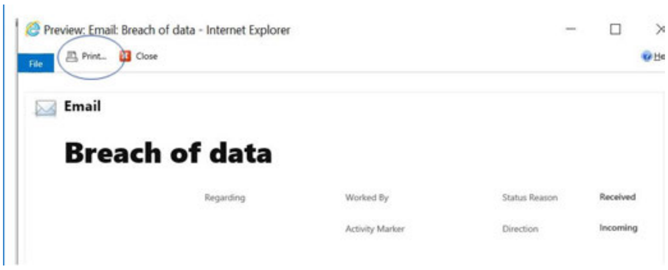
Downloading items from ICE

- Open the sift item.

- On the top right hand corner of your ICE360 screen in the blue navigation bar, select the cog and click 'Print Preview'



- When the box opens click the print button (circled). When the print box opens, chose 'Microsoft Print to PDF'.



- This will then let you save the document to your desktop and then it can be emailed to the s.31 [redacted] inbox.

DELEGATED WHISTLEBLOWING OFFICERS ONLY

- Email is received into [redacted] inbox.
- Postal correspondence is received via internal post from scanning.

DETERMINE WHETHER THE CASE IS WHISTLEBLOWNG

- Before creating a case in SharePoint you should determine whether the correspondence falls under whistleblowing legislation.
- The correspondence should be dealt with as an normal course of business enquiry if:
    - The individual is not an employee/ex-employee.
    - The enquiry/complaint concerns the individuals' own personal data.
    - The name/identity of the data controller concerned is not identified.
- Create an advice case in ICE and respond, including a definition, explanation or link to whistleblowing guidance.

SETTING UP A WHISTLEBLOWER CASE

Check for existing cases

- Open whistleblower RA SharePoint site.

- Search Whistleblower Admin Log for existing cases from this whistleblower.

- If no existing case, complete log with details of new case as follows:
    - date received
    - case reference number (reference generated in following format 'SPWnnn', where nnn represents the sequential number of the item received)
    - case officer (delegated officer name)
    - regarding (name of DC whistleblower report relates to)
    - status (open or closed).
- Save.

- If an existing case exists, ensure the documents are saved in the relevant folder on SharePoint.

Creating a case

- On whistleblower RA SharePoint site, go to relevant month sub-site.
- Within month sub-site, select '+New'
- Select 'WB Case Folder' to create a new case.
- Complete details on case as follows:
    - name (ref: SPWnnn)
    - channel received
    - date received
    - sector
    - WB Case Status (open)
    - security clarification (official – sensitive)

Upload documents to the case

- Once case created, save email from [redacted] inbox to desktop.
- Rename email(s) as per naming conventions at Appendix.
- Drag and drop email from desktop into newly created case.
- Check email has saved before deleting email from desktop and [redacted] inbox.
- Repeat for any other emails relating to that case.

ACKNOWLEDGING WHISTLEBLOWING CASES (EMAIL)

Replying

- Open email from wb case.
  (Email will then open as separate outlook message)

- If email has come direct from whistleblower
    - use the reply function.
- If email is forwarded email from another inbox
    - click reply
    - manually copy and paste the email address of the whistleblower into the 'To' field.
- If wb form was completed by helpline staff, if an email address was provided by the whistleblower we can send an acknowledgment. Particular care must be taken to cross check email address with completed form.

Email

- Add case reference number (ie SPWnnn) to subject line.
- Change 'From' field so email is sent from [redacted] email address.
    - select 'Options'

- Select ‘From’.
- Select [redacted]

(The first time you do this you will need to manually add [redacted])

- Draft acknowledgement email using WB template – initial acknowledgment.
  (You can access the WB templates through the whistleblower RA SharePoint site)

Admin

- Ensure privacy notice and email signature is included.
- Check email address against original correspondence and send.
- Add email security check to case log.
- Go to sent items on outlook.
  - Save email from sent items to desktop.
  - Rename email as per naming conventions.
  - Drag and drop sent email from desktop to wb case.
- Check email has saved to SharePoint before deleting email from desktop and sent items.

ACKNOWLEDGING WB CASE (POSTAL)

Draft

- Draft letter in word using WB template – initial acknowledgement.
- You will need to add:
  - postal address,
  - reference number
  - date.
  - Privacy notice (website address)

Admin

- Check postal address against original correspondence.
- Add address security check to case log.
- Save document to desktop as per naming conventions.
- Drag and drop letter from desktop to wb case.
- Check letter has saved to SharePoint before deleting letter from desktop.

REFERRING CASE TO INTELLIGENCE HUB

Email

- Create new email in outlook to [redacted]@ico.org.uk.

- Change 'From' field so email is sent from [redacted] email address.
- Draft referral email using – WB template – IH Referral Email.
- Send email.

Admin

- Save email from sent items to desktop.
- Rename email as per naming conventions.
- Drag and drop sent email from desktop to wb case.
- Check email has saved to SharePoint before deleting email from desktop.

Intelligence Hub

IH will check Whistleblowing RA SharePoint site and view documents.

The information will be logged on the intelligence recording log in a sanitised format. The sanitised information will make no reference to the source, with no gender specifics and no reference to how or where the information was obtained.

Entering the sanitised information on the Intelligence Recording Log will generate a unique reference number (URN) (in the format yyyymmddnn where nn is the sequential number of the item of the day). A grading should also be recorded for the information evaluating the source, information and handling in accordance with the National Intelligence Model.

Intelligence will add their URN to the whistleblowing admin log on the whistleblowing RA SharePoint site.

FOLLOW UP CORRESPONDENCE

Any follow up correspondence from the whistleblower or from IH should be added to the case. It is the responsibility of the delegated officer who created the case to acknowledge any further correspondence, even if it is not their week on the inbox.

The delegated officer on the inbox should follow the below process to alert the owner of the case of the new correspondence.

- Delegated officer on inbox to save email to desktop.
- Rename email as per naming conventions.
- Drag email into relevant case.
- Check email has been saved to SharePoint before deleting email from desktop and inbox.
- Email delegated officer owner (name should be on spreadsheet) to notify of new correspondence.

- Save email to delegated officer owner to case.
- Case owner may use the various templates for follow up response replies which can be found in the Admin Log Library area of the RA SharePoint site.
- Please flag with [redacted] if the case owner is on leave for longer than one week, as a different process may need to be followed.

The case owner should flag any follow up correspondence which becomes protracted or indicates the whistleblower may be unhappy with their information being handled under this procedure.

INFORMATION REQUESTS

The majority of information requests should come through the normal whistleblowing procedure. Whistleblowers should however be encouraged, where possible to make any requests through the delegated officers.

- If you identify a request for information (SAR or FOI) it should be flagged with the Information Access managers (Ian Goddard)
- The IA team will then liaise with delegated officers to determine what information is held and falls within the scope of the request.

- Temporary access to the restricted area of SharePoint should be requested by a Group Manager using the Request for Access – Restricted SharePoint template.
- The form should identify:
    - The name of the officer.
    - The reason for access.
    - The length of the access required.
- The completed form should be sent to [redacted]@ico.org.uk
- marked for the attention of Danielle Haslehurst.
- The delegated officer in IA will then deal with the information request through the restricted SharePoint site.

Appendix - Naming conventions

Item	Naming convention
Completed whistleblowing form	Completed whistleblowing form
Initial email from whistleblower	WB to ICO (initial report) [DATE] [TIME]
2nd /3rd initial email from whistleblower	WB to ICO (initial report2/3) [DATE] [TIME]

Acknowledgment email/letter	ICO to WB (acknowledgement) [DATE] [TIME]
IH referral email	ICO to IH (internal IH referral) [DATE] [TIME]
Response from IH	IH to ICO (internal correspondence) [DATE] [TIME]
Response/chaser from whistleblower	WB to ICO (response/chaser) [DATE] [TIME]