Information Commissioner’s Office

Internal Audit Report: Case Management

January 2023

FINAL REPORT

mazars

Contents

Disclaimer

This report ("Report") was prepared by Mazars LLP at the request of the Information Commissioners Office (ICO) and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit the ICO and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix A1 of this report for further information about responsibilities, limitations and confidentiality.

01 Introduction

As part of the agreed Internal Audit Plan for 2022/23, we have undertaken a review of the Information Commissioner's Office (ICO) key controls for case management. The scope of this audit focused on the following key areas:

- Case management policies and procedures;
- Staff training and awareness;
- ICE Access;
- Quality assurance checks;
- Complaints/feedback; and
- Reporting.

Full details of the risks covered are included in **Appendix A1**.

As agreed with the Director of Corporate Planning, Risk and Governance, this audit has focused on cases managed by the Public Advice and Data Protection Complaints Department as this department investigates the majority of complaints the ICO receives. As part of the audit, we have not reviewed whether the correct decision has been made on cases or that the relevant legislation applied is correct.

We are grateful to the Team Manager, Group Manager, Director of Public Advice and Data Protection Complaints Service, Head of Public Advice and Head of Data Protection Complaints, along with other staff for their assistance during the audit.

This report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Any such matters have been discussed with the relevant staff.

02 Background

A key part of the ICO's role is to record and consider concerns raised around the handling and misuse of personal data that has been reported by the public. Since the implementation of GDPR, the intake of cases into the Public Advice and Data Protection Complaints Department has significantly increased. In the last 12 months, the department has received 33,000 cases. As of January 2023, there are 4,457 active cases, 724 of these cases are over 90 days old (16.2%).

The department has approximately 200 staff. Case Officers attend Training School before being assigned to one of the six data protection groups:

- charities, education and media;
- lenders, credit reference agencies, transport, health and use of domestic CCTV;
- local Government, London Boroughs, housing;
- police, justice and prisons;
- general business and retail; and
- central government, political parties, internet and insurance.

Once a data protection complaint is raised, it is recorded on the case management software, ICE 360, which was implemented in April 2020. Complaints relating to data protection should be handled in line with the Complaint Handling Procedure. Cases are assigned to a Case Officers work queue, where they are required to add the relevant legislation, the case will be reviewed under: UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

The case management process followed depends on the type of complaint but includes an investigation by the Case Officer to make a decision whether there has been a breach of legislation.

Access to the ICE system is granted when a Case Officer is assigned to one of the relevant groups. The system is accessed via desktop app. Training videos on ICE are available for staff to view on SharePoint.

A Quality Assurance Framework in place for case management. The framework dictates that managers should quality assure at least three cases per Case Officer per quarter. If a complaint is made regarding the service received, they are handled in line with the Service Complaints Policy. If a complaint is made about a decision outcome, this is subject to a manager review.

Case management performance is monitored within management information reports which are stored on SharePoint for all staff to access. Each month, a report is issued to senior management containing performance data including cases outstanding and age profile. Quarterly reports are presented to the Management Board. Performance for Q2 was last reported in November 2022 as follows:

Measure	Quarter 1	Quarter 2	RAG status
We will assess and respond to 80% of Data Protection concerns within 90 days	46%	53.5%	Red
We will assess and respond to 90% of Data Protection concerns within 6 months	94.1%	96.6%	Green
Less than 1% of our Data Protection complaints caseload will be over 12 months old	0.5%	0.3%	Green
We will resolve 80% of written enquiries within 7 calendar days	81%	83.8%	Green
We will resolve 99% of written enquiries within 30 calendar days	96.9%	97.2%	Amber
In 100% of cases, the Parliamentary and Health Service Ombudsman (PHSO) do not uphold a complaint about the ICO	100%	91%	Amber
We will investigate and respond to 90% of service complaints within 30 calendar days	72.5%	85.4%	Amber

As the ICO is significantly behind target in relation to responding to 80% of concerns within 90 days, the following actions have been taken:

- Reports on case volumes, age profile, cases allocated, and cases completed are updated daily and available to managers on SharePoint.
- Weekly performance meetings are held with a representative from each group. Case volumes and age profile are discussed, and decisions made on the number of cases to be allocated.
- The management team have considered potential efficiencies, such as providing faster initial responses in order to reduce double handling of cases.

There has been a steady improvement in performance since Quarter 1 from 46% to 53.5%. Data provided as of 12 January 2023 highlights the number of Data Protection concerns responded to within 90 days is 64%, demonstrating ongoing improvement.

03 Key Findings

Assurance on effectiveness of internal controls

● Adequate Assurance

Rationale

The internal audit work carried out has provided **Adequate Assurance**. Please see Appendix A1 for the detailed scope and definitions of the assurance ratings.

Our audit has identified three key areas of improvement in relation to the usability of the ICE system, recording of case decisions and consistency of completing quality assurance checks.

Please see **Section 04** for further detail in respect of the recommendations made from our review.

Number of recommendations

High	Medium	Low	Total
-	3	4	7

3.1 Examples of areas where controls are operating reliably

- We confirmed via screenshare that the ICE 360 DP Complaints Handling Process and training videos for casework are available for staff to view on SharePoint. These process documents and training videos provide information and guidance on case handling and the use of the ICE system. (N.B., We have raised a recommendation in relation to the update of the process document in Section 04).
- We reviewed the job description for Caseworkers and confirmed this clearly included roles and responsibilities in relation to case management.
- Staff receive training on case management and the ICE system at Training School, and via a series of training videos available to them on the intranet. We issued a survey to 181 ICE users in the Public Advice and Data Protection Complaints Department and received 105 responses. Of the staff who responded, 71% agreed that the training they have received on the ICE system is sufficient for their role.
- Staff access the ICE system as an application through their staff login. ICE software is assigned to the relevant users and available through desktop access. We reviewed ICO password requirements and confirmed that these are in line with National Cyber Security Centre guidance. Passwords must have a minimum of nine characters, which should include a mixture of upper- and lower-case letters, numbers and special characters.
- We selected a sample of 15 data protection cases between February 2022 and September 2022. In line with the ICE360 DP Complaint Handing Process we confirmed:
  - All cases were assigned to the correct sector group;
  - Key data logged on ICE matched the original case data;
  - All cases had legislation recorded on ICE (DP18/UKGDPR);
  - In all cases, the complainant had been contacted to advise them of the case closure; and
  - In all applicable cases, the data controller had been contacted.
- Case management performance is monitored within Management Information (MI) reports. The reports include a list of open cases and the age profile. We confirmed these reports are available in SharePoint to view and automatically updated weekly. (N.B we were unable to test the accuracy of the figures as this data is produced from a pre-built SQL report built into the data warehouse.

Recalculating the reported figures to the source data would require development of another SQL query.)

- Quarterly reports are presented to the Management Board. As the ICO is significantly behind target in relation to responding to 80% of data protection concerns within 90 days (46% at Quarter 1 and 53.5% at Quarter 2) the following actions have already been taken by the ICO:
    - Reports on case volumes, age profile, cases allocated, and cases completed are updated daily and available to managers on SharePoint.
    - Weekly performance meetings are held with a representative from each group where case volumes and age profile are discussed and decisions made on the number of cases to be allocated. These meetings are not minuted but we viewed calendar invites to confirm the existence.
    - The management team have considered potential efficiencies such as providing faster initial responses to reduce double handling of cases.

  Data provided as of 12 January 2023, highlights the number of Data Protection concerns responded to within 90 days is 64%, demonstrating ongoing improvement.

3.2 Risk Management

The ICO has no direct risks in its Risk and Opportunity Register that relate to the audit scope around data protection complaints or case management. Our review found some medium priority issues with the recording of Decision Reports on cases, with some incorrectly recorded or no decision present. As this can directly impact the ICO's ability to investigate or undertake regulatory action, we have raised a recommendation in relation to this in Section 04.

The Public Advice and Data Protection Complaints department has its own directorate risk register. There are no direct links to case management or reference to the ICE system, instead this contains the following risks relating to staffing:

- Lack of capacity; and
- Lack of capability.

Given that the department experience some functionality issues with ICE360, the ICO may want to consider inclusion of the ongoing ICE improvement project to the directorate risk register. Improving functionality issues with ICE may positively improve capacity and capability issues within the department through efficiencies.

3.3 Value for Money

Value for Money can often be difficult to derive in a case management context due to the fact the nature of activity is extremely varied depending on the complaint at hand.

The use of case management systems can help to reduce the burden of manual monitoring and management of cases and progress. Such systems can offer functionality of storing information and forms to enable quicker review processes where possible. The ICO implemented ICE software as a case management system in April 2020.

We completed an employee survey that highlighted staff dissatisfaction with ICE as a case management system and highlights potential issues with its functionality. We asked staff how much time they spend per day using systems outside of ICE as a workaround to functionality issues. 66% of respondents stated they spent over one hour per day using such workarounds, indicating that the system may not be providing value for money.

During the course of the audit, we were advised that improvements to the system regarding casework were put on hold until a wider piece of work to upgrade the system has been completed. The ICE system is also used by other departments in the organisation. The upgrades are expected to be completed in December 2022.

Results of the staff survey are available in Appendix A2, and we have raised a recommendation in Section 04.

3.4 Sector Comparison

At peers, we see case management systems bring benefits such as:

- Data kept in a single, central location that is easily accessible. Less time is therefore spent looking for key documents;
- Functionality for data analysis, enabling trends and patterns to be identified;
- Enhanced management oversight over case progress; and
- Improved compliance with data retention requirements.

Whilst ICE allows the department to store data in an accessible, central location, low scores in the staff survey were received on questions relating to ICE's ability to track and manage officer caseload, which is a key function of a case management system (See Appendix A2). The ICO use live SQL reports set up in the data warehouse in order to monitor trends and patterns. Data is updated daily and available for staff to view in SharePoint.

04 Areas for Further Improvement and Action Plan

Definitions for the levels of assurance and recommendations used within our reports are included in **Appendix A1**.

We identified areas where there is scope for improvement in the control environment. The matters arising have been discussed with management, to whom we have made recommendations. The recommendations are detailed in the management action plan below.

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
4.1	**ICE Software** Data protection complaints are logged and managed within the case management software, ICE, which was implemented in April 2020. Staff have reported functionality issues regarding ICE and the ICO is aware of these issues. Improvements to ICE are currently paused until April 2023 pending a larger piece of work for the organisation as a whole to upgrade ICE. Users have reported issues with the formatting of emails, attachment of documents to ICE and tracking of cases. We issued a survey to 181 ICE users and received 105 responses. Some of our questions related to ICE and asked staff to rate their agreement with the following statement on a five-point scale (1 - Strongly disagree to 5 - strongly agree). The feedback on the ICE system was generally negative or neutral with the following results: • 'The ICE system is easy to use' – 38% of respondents disagreed with this statement. • 'The ICE system provides helpful information to help me to track and manage my team's caseload' - This statement was aimed at Managers only. 60% of respondents disagreed with this statement. • 'ICE has the functionality I need in order to manage my cases effectively and efficiently'. 42% of respondents disagreed with this statement.	As planned, the ICO should implement the improvements to the functionality of the ICE system. This should include improvements to its case tracking functionality and resolve issues with formatting of emails and attaching documents. The ICO should complete a cost v benefit analysis of the ICE system to assess whether it is ft for purpose and is supporting the achievement of value for money.	**Medium**	The functionality issues highlighted by this report form part of a wider Digital and IT transformation piece. We note the recommendation to proceed with this piece of work and agree that it would improve the process for all ICE users. However, we also note and agree with the further recommendation to conduct a cost v benefit analysis of the ICE system. This analysis will help inform how best to address functionality issues.	March 2024 Mike Fitzgerald, Director of Digital, IT and Business Services

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	We also asked staff how much time they spend per day using systems outside of ICE as a workaround to functionality issues. 66% of respondents stated they spent over one hour per day using such workarounds. *Risk: The case management system is not fit for purpose. Staff are not able to maximise productivity due to functionality issues with the system.*				
4.2	**Decision Reports** All data protection complaints are required to be closed with a Decision Report. The Decision Report records the relevant decision, action, notice and legislation with which the complaint has been handled. Any cases or reviews that are closed without Decision Reports are flagged on an exception report, which is updated weekly in SharePoint. There is a particular focus to resolve this on a quarterly basis for reporting purposes, however, we were informed these are not always completed within the quarter. The exceptions report for December 2022 highlighted: • 7 cases with incorrect notices; • 64 cases with no Decision Report; • 151 cases with no legislation reason recorded on Decision Report; • 165 cases with no action on Decision Report; and • 148 Cases with no decision recorded on Decision Report. *Risk: Decisions on cases are not recorded or recorded incorrectly, affecting performance figures as well as decisions on investigations and formal regulatory action.*	The ICO should: • Implement more regular reviews of Decision Report exceptions (e.g. monthly); • Conduct a trend analysis to identify whether lack of Decision Reports is affecting particular officers or teams; and • Issue a reminder to all officers of the importance of attaching Decision Reports to cases.	**Medium**	As noted in the observation/risk notes, exception reports are produced monthly. We agree with the recommendations to focus our attention on improving this aspect of the work. We will provide a reminder to our teams about the importance of completing Decision Reports. The management team will also review their group adherence, and then conduct more routine reviews of the reports.	10 Feb 2023 – reminder to teams to complete the reports. 31 May 2023 – complete group analysis of current adherence From this date start to conduct more routine review of exceptions. Faye Bower, Head of Public Advice Services
4.3	**Quality assurance (QA)** Management informed us that each casework officer should be subject to QA reviews of three cases per quarter, to	The ICO should: • Update the explanatory notes to	**Medium**	Alongside QA, line managers and reviewing officers will routinely conduct case reviews, or respond to service	30 June 2023 Helen Raftery

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	ensure quality of casework. This should be completed using a QA Evaluation Form. The QA ratings are either Pass, Pass with Feedback or Not Passed. The ICO has explanatory notes in place for using this form, which state that if a caseworker receives a ‘Not Passed’ rating, they should be subject to additional QA. However, the notes do not outline what specific steps should be taken if a case review does not pass, nor do they dictate the required frequency. QA Evaluation Forms are recorded by the line manager, and results are not recorded in a central location for development purposes. We selected a sample of 12 staff members, two from each of the six data protection groups to confirm three case reviews in the last quarter have been completed. We found: • One group is not currently completing QA reviews; • One group was only completing QA checks when a case had been subject to a decision review; • Four staff across teams had not had a QA check. We were informed this was due to ‘manager decision’; • One case review where a ‘Not passed’ result had been recorded in October 2022, however, the officer had not been subject to additional QA since. *Risk: The ICO does not monitor the quality of how cases are managed or responded to, leading to a poor service and improvements not identified.*	include required frequency of reviews and what steps should be taken in the event of a non-pass QA; • Communicate the updated explanatory notes to Line Managers; and • Ensure QA is completed in line with agreed requirements and use the results to drive improvements in service. QA results should be recorded and reviewed centrally.		complaints. This provides an additional level of scrutiny to the quality of our work. We note the recommendations to further strengthening our QA process and will update the explanatory notes. We will give further consideration as to recording this information centrally. It is important that we retain information in line with service standards, and that we do not inappropriately divulge customer or case officer information. We will however ensure that we introduce a mechanism to ensure that overall recommendations are shared to provide opportunities to improve service.	Acting Head of Data Protection Complaints
4.4	**Complaints** If a complaint is made regarding the service received from the ICO, it will be handled in line with the Service Complaints Policy. The ICO has a KPI to monitor timeliness of responding: ‘to investigate and respond to 90% of the service	The ICO should: • Determine set timescales for responding to complaints about	**Low**	We take complaints about our service and decision making seriously and agree with the importance of learning from complaints.	30 Sept 2023 Faye Bower, Head of Public Advice Services

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	complaints within 30 calendar days'. The ICO is currently behind target at 85.4% in Q2, however, performance has significantly improved since Q1 at 72.5%. If a complaint is made about a decision outcome, this is subject to a manager review. There a no pre-defined timescales to responding to these complaints. We selected a sample of five cases from February 2022 to September 2022 which had been raised in relation to a decision outcome and confirmed all had been subject to a manager review. In all five occasions there was an acknowledgement within 14 days of the complaint. The average final response rate from the acknowledgement was 21 days (one complaint took 37 days to be responded to). We note that neither the Service Complaints Policy or the Complaint Handling Process detail how complaints or feedback are used to drive improvements in the service. Lessons learnt for each complaint are not identified and documented. We understand that this is a more informal process at present. *Risk: Complaints regarding decision outcomes are not responded to in a timely manner due to lack of defined timescales. The ICO does not utilise complaints and feedback to improve its service.*	decision outcomes and monitor against these; and • Develop a formal process to identify, document and implement lessons learnt from complaints. The ICO should also review themes arising from complaints about the service to identify any wider service improvements.		We endeavour to respond to complaints about our decision making swiftly but note the recommendation to include a timescale. Complaints about decision making, and complaints about our service, affect other areas of the business and there is a need for consistency. This will therefore be subject to wider consideration.	
4.5	**ICE Access** We compared a list of current staff to a list of ICE users in the Public Advice and Data Protection Complaints Department and found three staff members who had left the ICO but had not had their ICE access disabled. The Team Manager informed us that upon a staff member leaving, a leaver form is sent to IT who should disable access to key systems including ICE.	The ICO should ensure all leavers are removed from the ICE system when employment ceases.	**Low**	We agree with this recommendation. As the leavers process is ICO wide, we will work with IT and People Services colleagues about how best to implement the suggested change.	31 May 2023 Mike Fitzgerald, Director of Digital, IT and Business Services

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	We note that the risk is mitigated here due to the ICE system only being accessible via the desktop and not as a cloud system. *Risk: Staff have access to ICO systems and data after leaving employment.*				
4.6	**Staff training** New caseworkers are required to undertake an initial period of training with the ICO's Training School. Training is not formalised or recorded, with caseworkers provided with the ICE system training videos and requirements to shadow members of staff. The staff survey completed as part of the audit (See Appendix A2) highlighted that 71% of staff agree that the training they received on ICE is sufficient for their role. *Risk: Staff are unaware of their responsibilities in relation to case management leading to poor service levels.*	The ICO should consider introducing a training checklist for new staff, to ensure they have covered key areas of casework training and there is a record.	**Low**	We have various existing checklists as part of our PADPCS training manual, which include ensuring that new starters satisfactorily complete key casework and ICE training. We will however review these in view of the recommendation.	31 May 2023 Faye Bower, Head of Public Advice Services
4.7	**Process document** The document 'Business process – ICE 360 - complaint handling procedure' was drafted to support the implementation of the ICE software in April 2020. The procedure document has not been reviewed since and there is no programme of regular review, however, we found in our areas of testing that current practice is in line with the procedure document. *Risk: Staff are unaware of how to carry our tasks correctly due to incorrect process documents.*	The ICO should review its process documents and set a programme of regular review.	**Low**	We note this recommendation. The overall document is an ICO wide one and so will share this with colleagues. We will also introduce a review process to areas that are PADPCS specific.	30 September 2023 Faye Bower, Head of Public Advice Services

A1 Audit Information

Audit Control Schedule	
Client contacts:	Suzanne Gordon, Director of Public Advice and Data Protection Complaints Service Faye Bower, Head of Public Advice Andrew Laing, Head of Data Protection Complaints Ian Johnson, Team Manager – Public Advice and Data Protection Complaints Service
Internal Audit Team:	Peter Cudlip, Partner Hannah Parker, Manager Jessica Holt, Assistant Manager
Finish on site/ Exit meeting:	12 December 2022
Last information received:	22 December 2022
Draft report issued:	13 January 2023
Management responses received:	16 January 2023
Final report issued:	27 January 2023

Scope and Objectives

Audit objective: To provide assurance over the design and effectiveness of the key controls operating in relation to the ICO's case management. Our review considered the following risks:

- **Case management** – The ICO does not have adequate policies and procedures in place to guide case management. Cases are managed inconsistently or incorrectly, resulting in poor service and delays in resolution.
- **Staff training and awareness** – Staff are unaware of their responsibilities in relation to case management leading to poor service levels. Staff have not been trained on case management or the ICE system and therefore the functionality of the system is not fully realised.
- **ICE Access -** Access to the ICE system is not limited to appropriate staff members. Password access for the ICE system is not suitably restricted.
- **Quality** – The ICO does not monitor the quality of how cases are management or responded to, leading to a poor service and improvements not identified.
- **Complaints/feedback –** The ICO does not have a process for receiving feedback or complaints on its handling of advice and formal complaints. Complaints and feedback are not used to drive improvements in the service.
- **Reporting –** The ICO does not record and monitor key performance data in relation to case management. Reported figures are inaccurate and senior management are not aware of performance issues and backlogs. Actions are not identified to improve performance where required.

The scope for the audit is concerned with assessing whether the ICO has in place adequate and appropriate policies, procedures and controls to manage the above risks. We will review the design of controls in place and, where appropriate, undertake audit testing of these to confirm compliance with controls, with a view to forming an opinion on the design, compliance with and effectiveness of controls. Testing will be performed on a sample basis, and as a result our work does not provide absolute assurance that material error, loss or fraud does not exist.

Definitions of Assurance Levels	
Level	**Description**
Substantial	The framework of governance, risk management and control is adequate and effective.
Adequate	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Definitions of Recommendations		
Priority	**Definition**	**Action required**
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.

Statement of Responsibility

We take responsibility to the Information Commissioner's Office (ICO) for this report which is prepared based on the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

A2 ICE User Staff Survey

As part of the audit, we shared an online survey with Public Advice and Data Protection Complaints Department staff via Slido. The purpose of the survey was to quantify user experience with the ICE360 case management system. We provided staff with a series of statements and asked them to rate their agreement on a five-point scale, from Strongly Disagree (1) to Strongly Agree (5). We received 105 responses and have detailed these below.

From the survey, we identified that users, both casework officers and managers, do not find ICE's functionality in relation to case management helpful. We also noted mostly positive results in relation to training on the ICE system.

Question	1 Strongly Disagree	2	3	4	5 Strongly Agree	Average Rating
The training I have received on case handling is sufficient for my role	1%	6%	11%	27%	**55%**	**4.3**
I am clear on my responsibilities in relation to case handling	0%	2%	7%	26%	**66%**	**4.6**
The training I have received on the ICE system is sufficient for my role	2%	4%	23%	33%	**38%**	**4**
The ICE system is easy to use	18%	20%	**37%**	20%	5%	**2.7**
The ICE system helps me to track and manage my caseload (*This question was aimed at Caseworker Officers and Lead Caseworker Officers)*	17%	14%	25%	**29%**	14%	**3.1**
The ICE system provides helpful information to help me to track and manage my team's caseload *(This question was aimed at Managers only)*	**48%**	12%	28%	8%	4%	**2.1**
ICE has the functionality I need in order to manage my cases effectively and efficiently	21%	21%	**30%**	21%	8%	**2.7**

Contacts

Peter Cudlip
Partner, Mazars
peter.cudlip@mazars.co.uk

Hannah Parker
Manager, Mazars
hannah.parker@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 44,000 professionals – 28,000 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.co.uk