

# Lincolnshire County Council

## Information Assurance

Annual Report  
2020/21

# Contents

**Foreword** Page 3

---

**Executive Summary** Page 4

---

**Data Protection** Page 5

---

**Records Management** Page 7

---

**Information Security** Page 9

---

**Appendix 1 - Key risks** Page 11

---

**Appendix 2 – External Engagement** Page 12

---

# Foreword

Information assurance (IA) is a cornerstone of any organisation that relies on information to deliver its services, particularly that of local government which collects and uses such diverse and sensitive information.

Done well, IA supports effective governance and ensures that the council understands, and aligns with, the legal and regulatory environment within which it operates by using information in a way which is lawful, fair, transparent, and secure.

A council that projects a digital vision of future council services must have confidence in the people, processes and technology responsible for delivering this vision. The need for confidence in the delivery of services also extends to members of the public, and our strategic partners as it helps to ensure opportunities are maximised by encouraging engagement through digital channels.

IA helps the council to achieve this by implementing a corporate framework designed to support colleagues, including information owners, to better understand information risk and to encourage informed decision making.

This annual report summarises activity undertaken by the IA Team during 2020/21 and reflects the output of 3 core specialist areas delivered by 11 IA staff.



David Ingham  
Head of Information Assurance  
07876 148551  
David.Ingham@lincolnshire.gov.uk

# Executive Summary

Unsurprisingly 20/21 was dominated by our response to COVID-19 as we adapted the delivery of the IA service to ensure support for colleagues remained at a high level.

Increased flexibility was necessary, particularly in the early stages of the wider council's response, as exceptions to normal council practice and policy were needed. This required a robust and transparent risk managed approach that enabled and supported delivery of frontline services..

An increase in new data flows, and data sharing, predominantly in the area of Public Health, also presented new challenges as we responded to immediate requests for support and advice on a rapidly changing basis. Our response ensured that colleagues were provided with timely advice which assisted the free flow of data.

Alongside the response to COVID-19 normal IA activity continued with enhancements to a wide range of controls. Reassuringly we continue to see positive engagement from colleagues across a variety of services who seek support from the IA team.

It can be reported that, except for the legacy records management project, there was no interruption to the IA service at any point over the last 12 months.

---

## 5 Key Assurance Messages

- The single biggest risk to the council remains a successful cyber attack which results in significant or critical negative impact to the council.
- Continued close engagement with technical colleagues within the councils IMT function and Serco, have led to direct improvements to our cyber security posture. However key areas, such as unsupported software, require significant effort to resolve.
- The records management legacy hard copy records project, following sizeable challenges due to COVID-19, refocussed efforts on activity which could be achieved within social distance guidelines. This resulted in positive outcomes which continued to reduce risks relating to legacy records.
- Data protection services continue to demonstrate value in supporting colleagues to deliver effective services. Engagement across the council remained high. In addition to ad hoc support IA provided extended support to more than 150 projects/tasks.
- The total number of reported security incidents for 20/21 fell by 12% compared to the previous year, with onward reporting of data breaches to the Information Commissioners Office falling by 41%.

# Data Protection

## Summary

Over the last 12-month data protection services have played an important role in supporting the delivery of the councils COVID-19 response. Despite the fast-paced and rapidly changing environment, the service was able to respond quickly to changes in legislation and regulation to ensure that personal data was processed appropriately and in line with third party requirements.

At the same time, the service continued to improve visibility of personal data held by the council and enhanced corporate controls designed to improve accountability.

---

## Key Headlines

- Supported Public Health colleagues to ensure the council demonstrated accountability for personal data provided by Public Health England as part of our COVID response. This included the development of information sharing agreements and contract/project support.
- Initiated a full review of surveillance camera systems across the council to support our responsibilities under the Surveillance Camera Code of Practice. Visibility of such systems has improved significantly allowing follow on work to be undertaken.
- Established and mitigated risks relating to the outcome of Brexit including international transfers of personal data.
- Successfully submitted the NHS Data Security and Protection toolkit ensuring uninterrupted access to key health data.
- Completed work which introduces a common identifier across key information assets, allowing easier identification, support and control.
- 92% of colleagues successfully undertook IA E Learning. The highest total ever achieved.

---

## Key Challenges and Future Focus

- Continue work related to the surveillance camera review to further improve the council's compliance with related legislation and code of practice.
- Improve the council's response to the upholding of individual rights concerning personal data and to highlight the support available from the councils Data Protection Officer.
- To promote early engagement of the service to allow improved capacity planning and quality of response.
- To refine prioritisation of support to ensure we provide comprehensive support to those who need it the most.

# Data Protection – Key Data



**23** data protection infringements raised with the Data Protection Officer.



**9** complaints reported to the ICO by members of the public.



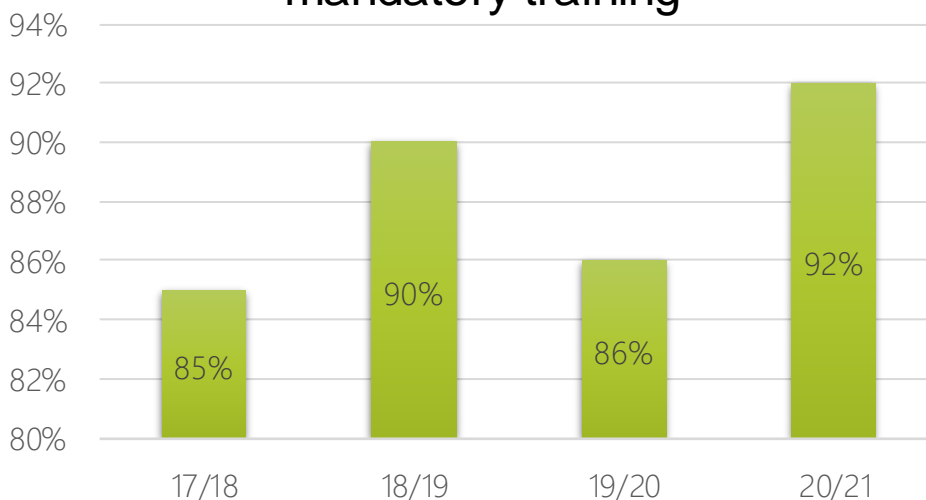
**9** complaints upheld or partially upheld by the ICO and **0** enforcement action



**156** projects/tasks requiring extended IA support

- 22% Adults and Community Wellbeing;
  - 21% Childrens
  - 17% Place
  - 16% Resource
  - 13% Commercial
- 10% Fire Rescue and Public Protection

## IA E Learning completion - mandatory training



# Records Management

## Summary

The key records management project designed to review hard copy records was subject to significant disruption due to COVID 19. As a result, the project refocused its efforts on work that could be achieved within social distancing constraints. This flexibility resulted in a different, but equally important, outcome improving visibility of records held. Work also continued to improve corporate controls.

---

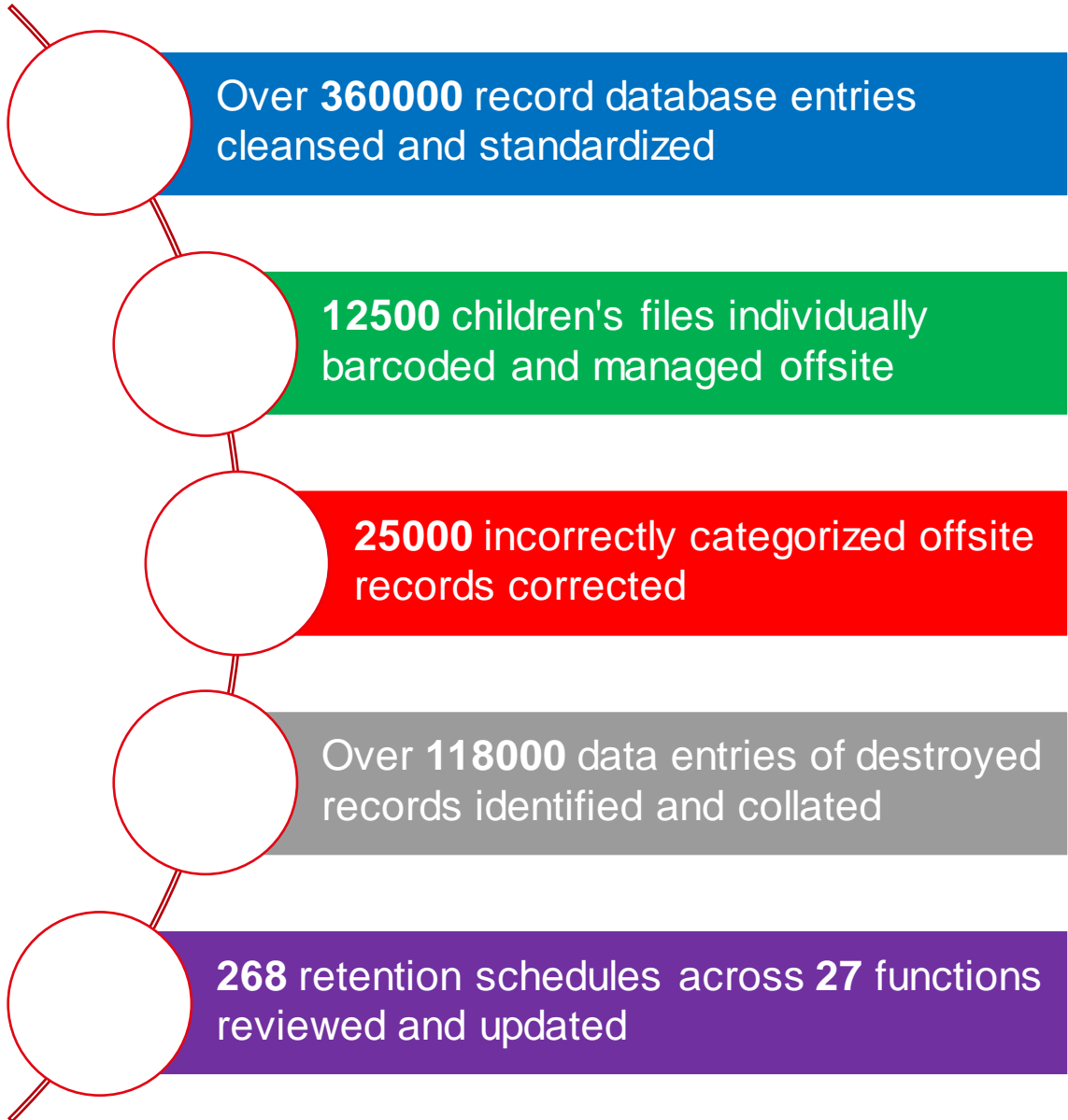
## Key Headlines

- Successfully introduced a functional classification scheme to assist in the mapping of records and content. It now supports a common thread across all IA activity. The scheme has been agreed by all information asset owners.
  - Reviewed and updated all corporate retention schedules to ensure they were accurate and reflected legal obligations and/or business need. These are now published externally to further demonstrate transparency.
  - Took advantage of a pause in the records management project to cleanse a significant number of individual offsite records to ease identification, assisting service areas to find records quicker.
  - Identified over 25000 records which were incorrectly categorised by our offsite storage provider. Successfully negotiated remediation cost reduction from £25K to £250.
  - Improved the records search process through better management and use of records management tools. This has directly led to the identification of previously lost service area records.
- 

## Key Challenges and future focus

- The current project to tackle legacy records on site will not achieve its aims within the current project timeframe with approximately 6000 boxes of records still to review on Lincoln campus alone. A bid to extend the timeframe of the current project is therefore necessary.
- Previously unknown historic issues with offsite records have been identified and will require additional attention to rectify. This must form part of the re-baselined hard copy records project.
- Smarter Working project and building rationalization engagement must be maintained to ensure principles of records management are applied. This reduces the risk of an increasing number of unmanaged records.
- Implementing an appropriate retention approach to Office 365 to support colleagues manage information effectively and to avoid historical issues presented by previous electronic solutions.

# Records Management – Key Data





# Information Security

## Summary

The council's enforced change to its working model because of COVID-19 required a swift and effective security response to ensure that risks remained manageable. The speed of change added an additional layer of complexity to the usual approach, but we are confident it was successful, evidenced by a reduction in the number of security incidents. Normal activity was maintained including continued assurance work across third parties and security investigations.

The scale and frequency of cyber attacks continued to present significant challenges and rebalancing the response remained a priority throughout the year.

---

## Key Headlines

- A 12% reduction in the number of confirmed security incidents, from 261 to 229.
- A 33% reduction in the number of data breaches reported to the Information Commissioners Office, from 12 to 8.
- Embedded Active Cyber Defence services, a National Cyber Security Centre programme, into the cyber assurance process helping to identify cyber risks across email, website, and network.
- An external audit of network security highlighted as good practice the IA governance in place which ensured “*..the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.*”
- Working in collaboration with technical colleagues in Serco and LCC IMT improved visibility and response to vulnerabilities present across the ICT environment. Response times have vastly improved.
- Supported the swift deployment of tools to support colleagues during COVID while still managing the risks they present, for example Zoom video conferencing and WhatsApp.

---

## Key Challenges and Future Focus

- Keeping pace with the cyber threat and the continual need for an “always on” response.
- Ensuring ongoing organisational awareness of the risks presented by malicious email while also supporting technical colleagues in improving the wider cyber security posture.
- Meeting capacity and knowledge demands borne out of an increased move to cloud services.
- Seeking out areas of improvement to reduce the number of security incidents.

## Cyber Attack Prevention



Over **100000** security events blocked on our network perimeter



More than **70000** malicious emails blocked.



Over **1 million** internet threats blocked



Over **1000** threats blocked on devices



More than **6000** security weaknesses identified and fixed

## Reported Security Incidents



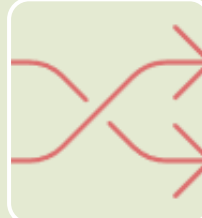
**229**  
confirmed  
security  
incidents



**88%**  
caused by  
human  
error



**90%**  
involving  
personal  
data



**81%**  
due to  
misdirected  
information




**3**  
successful  
cyber  
attacks

# Appendix 1 – Key risks

The IA Team manage risk concerned with cyber security; data protection; record's management and general IA. The table below reflects two key risks.

Risk	Raw rating	Current rating	Target rating	Risk travel
There is a risk of a <b>successful cyber attack</b> against the council which will have a <b>significant/critical impact</b> . (This risk is jointly owned by IMT)	16	12	8	

**Comment:** The cyber threat is constant and unrelenting. Significant attacks on Local Authorities and the Education Sector have demonstrated why it remains so relevant. Not only must the council prevent attacks but it must also be prepared to deal with successful attacks, which, unfortunately, are inevitable. We must therefore respond with a suite of technical and organisational controls designed to mitigate both the likelihood and the impact of cyber attacks. Sound organisational controls are in place, which remain under constant review, and improvements to technical controls have been implemented with a number ongoing. The nature of cyber security means it is an ever evolving picture with a need for ongoing investment and resource.

There is a risk that the council's legal obligations will not be met because of an <b>inconsistent and fragmented approach to hard copy records management</b> .	12	12	6	
--	----	----	---	---

**Comment:** This risk is largely due to the historic management of hard copy records resulting in dispersed holdings of uncontrolled records across the estate. A project was initiated in 2019 and is now in its final year. However COVID-19 has significantly hampered progress; this delay together with a significant number of holdings identified during the project means a project extension will be requested in 2021/22. Alongside project work improvements were made to a variety of corporate controls to improve how we manage hard copy records.

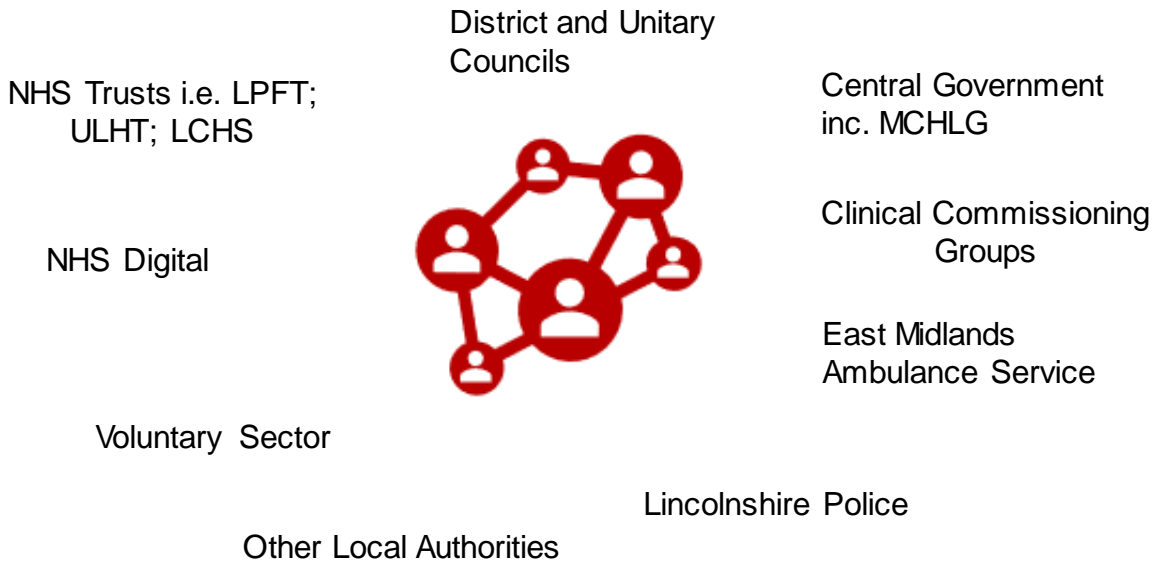
		Likelihood			
Key	4 Almost certain	4	8	12	16
	3 Probable	3	6	9	12
	2 Possible	2	4	6	8
	1 Hardly ever	1	2	3	4
Impact		1 Negligible	2 Minor	3 Major	4 Critical

# Appendix 2 – External Engagement

IA actively engages with a variety of external partners and agencies to support effective partnership working and knowledge sharing. This directly benefits the delivery of council services.

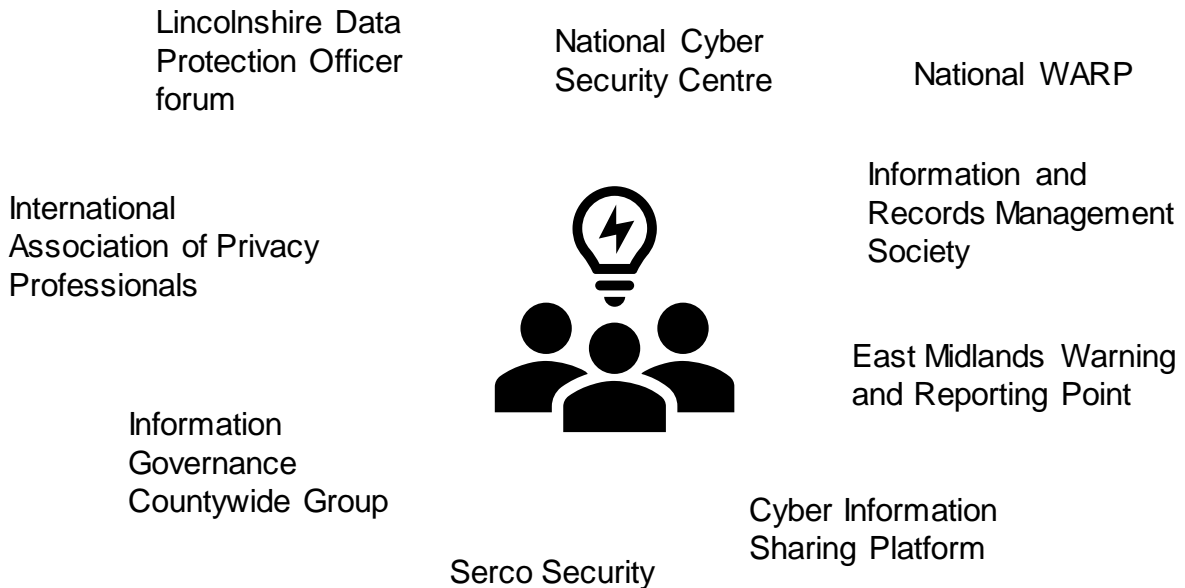
---

## Partnership working



---

## Knowledge Sharing



Serco Security Services