ESSEX POLICE, FIRE AND CRIME COMMISSIONER FIRE & RESCUE AUTHORITY
Essex County Fire & Rescue Service

Meeting	**ECFRS Performance & Resources Board**	**Agenda no.**	**8**
Meeting Date	**16 November 2022**		
Report Authors	**Ana Tuckwell, Information Governance Manager**		
Presented By	**Karl Edwards, Director of Corporate Services**		
Subject	**Audit of Information Governance**		
Type of Report	**Information**		
PFCC Action Point No.	**n/a**	**For Publication**	**Yes**

RECOMMENDATION(S)

The purpose of this report is to inform members of the ECFRS Performance & Resources Board of the findings of the recent audit as well as the action plan that went with the audit, Appendix A (Audit Report spreadsheet). Appendix B (S.212 process)

EXECUTIVE SUMMARY

The audit identified a number of areas for improvement which will be reviewed through the Information Governance Board for compliance, and this will subsequently be monitored through ECFRS Continuous Improvement Board (CIB).

BACKGROUND

An internal audit of all Information Governance processes and policies was conducted by the Data Protection Officer in March 2022. As a result, the overall rating was "Partially Compliant" with an action plan to achieve "Good Assurance".

Actions completed between August and November 2022):

- The IAOs have been established and they have received training on their responsibilities and accountability.
- The IG team has developed guidelines for processing information requests such as SARs FOIs EIRs and S.212. (Requests for police investigations to detect fraud or criminal activity)
- With the support of the Fire Investigation Team and Control, a process was put in place to handle S.212 requests. See Annex B
- All requests to exercise data protection rights are logged, categorised, and processed within the statutory timeframe.
- DPIAs template and process is now implemented.

What's going well:

- A new IG strategy have been developed, which will also be beneficial for Fire Standards Management.
- The Surveillance policy and procedure have been developed and will be discussed at the next IGB meeting.
- A framework for information governance has been established. There are still a lot of templates that need updating. In addition, the framework is one of the requirements of the Data Fire Standards.
- The Privacy Notices have been reviewed and updated; however, they must still be approved.
- Information Governance Team members are currently working with the IAOs on updating the Information Asset Register, Retention Schedule and RoPA (Record of an organisation's processing activities involving personal data. Pursuant to Art. 30 (3) GDPR)

What is remaining:

- Records Management: In the next three months, records management needs to be carefully considered. It's linked to risk number 6 in the legal implications section.
- Data Protection Awareness: A communication plan is being developed between the DPO and DDPO to raise data protection awareness.
- Technical Security documentation must be kept as a living document and reflected in IT policies.

The Audit report and action plan with progress can be found in Appendix A (Audit Report spreadsheet).

OPTIONS AND ANALYSIS

P&R Board to observe action plan and commit to the Service carrying out all actions needed to get us to a state of compliance.

RISKS AND MITIGATIONS

During the audit, seven risks were identified and entered into the risk register. This document contains a section on "*legal implications"* that describes each risk and the progress made from March to August 2023.

LINKS TO FIRE AND RESCUE PLAN

Digital & Data Strategy
Infrastructure and Security (Annual Plan)
Data Quality (Annual Plan)
Data Management Fire Standard

FINANCIAL IMPLICATIONS

Please include breakdown and any on costs if the matter is staff related.

LEGAL IMPLICATIONS

1. Contracts with suppliers and partners are not legally compliant, exposing the Authority to reputational damage, economic harm and regulatory censure. If legally compliant contracts are not in place, we can receive a financial penalty from the ICO. We cannot evidence compliance with the Accountability principle or articles 26 - 29 of the UK GDPR applied by the Data Protection Act 2018. **Action:** Risks have been mitigated. DDPO and DPO have updated templates and revised processes with Procurement Manager. They agreed on appropriate data processing agreement schedules. An end-to-end procurement process for staff has also been approved by the IGB and will be launched before the end of this year.
2. Surveillance is not managed in line with legal requirements and regulatory guidance which is likely to result in personal data breaches and render the Authority unable to meet the Accountability principle in the Data Protection Act 2018. This could lead to reputational damage and regulatory censure, including monetary penalties and claims for compensation. **Action:** The DPO and DDPO conducted a Surveillance audit. A draft of a surveillance policy and separate procedure document have been prepared and will be discussed on the next IGB.
3. The Authority is not transparent about its processing of personal data leading to regulatory censure. The law requires ECFRS to have clear privacy notices in place which cover all processing of personal data. This should be available on your website and signposted from all forms or activities where personal data is collected or used. **Action:** Risk have been mitigated**.** The privacy policy on the ECFRS website is now reviewed and published, however the other Privacy notices need to be reviewed.
4. Personal data could be shared inappropriately or unlawfully due poor understanding of legislation resulting in regulatory action or fines by the ICO, reputational damage or potential harm to individuals and claims for compensation. **Action:** Risk have been mitigated. There is an established template for information sharing protocols, and the DPO and DDPO are currently working on the implementation of a data sharing procedure.
5. Personal data is not actively minimised, which breaches the data protection principles. This happens when personal data is collected unnecessarily, for example because it is already held elsewhere in the Authority, or excess personal data is collected for a specific purpose, or personal data is duplicated across systems due to poor records management. Non-compliance with the data minimisation principle could result in reputational damage, regulatory censure and harm to individuals.
6. Personal data is not controlled, retained or destroyed in line with data protection law or the S46 records management code of practice. Records are stored across multiple storage areas, leading to duplication, inaccuracies and an inability to respond to statutory requests for information within legal timeframes. This may cause the Authority reputational damage, regulatory censure, increased workload, and damage the trust of staff, the public, and suppliers. **Action**: The retention schedule has been updated and will need to be approved by the IAOs.
7. Staff who manage information on behalf of the Authority (including volunteers) unknowingly breach data protection policies and guidance due to lack of awareness, communication and training. This can result in regulatory action or fines by the ICO, potential harm to individuals and claims for compensation.

Action: The risk has been mitigated. A module called *"Data Protection Essentials"* has been published in May 2022 to help staff fully understand their responsibilities. **1233** people have now completed the module, which is **83.6%** of the Service. DDPO has provided face-to-face data protection training.

STAFFING IMPLICATIONS

No staffing implications associated with this paper.

EQUALITY AND DIVERSITY IMPLICATIONS

We have considered whether individuals with protected characteristics will be disadvantaged as a consequence of the actions being taken. Due regard has also been given to whether there is impact on people who identify as being part of each of the following protected groups as defined within the Equality Act 2010:

Race	X	Religion or belief	X
Sex	X	Gender reassignment	X
Age	X	Pregnancy & maternity	X
Disability	X	Marriage and Civil Partnership	X
Sexual orientation	X		

The Core Code of Ethics Fire Standard has been fully considered and incorporated into the proposals outlined in this paper.

HEALTH AND SAFETY IMPLICATIONS

No health and safety implications associated with this paper.

CONSULTATION AND ENGAGEMENT

To include rep bodies, boards, external agencies

FUTURE PLANS

Make sure that all staff within ECFRS adopt best practices in accordance with relevant legislation to bring the Service into compliance.

LIST OF BACKGROUND PAPERS AND APPENDICES