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

Classification	**Official**		
Meeting	**ECFRS Performance & Resources Board**	**Agenda no.**	**13**
Meeting Date	**1st June 2023**		
Report Authors	**Ana Tuckwell, Information Governance Manager & DDPO**		
Presented By	**Karl Edwards, Director of Corporate Services**		
Subject	**Audit of Information Governance- update**		
Type of Report	**Information**		
PFCC Action Point No.		**For Publication**	**Yes/No**

RECOMMENDATION(S)

That the Board note the update on the action plan produced following the Data Protection Audit conducted by DPO in March 2022.

EXECUTIVE SUMMARY

Progress against the Data Protection Audit undertaken in March 2022 has been monitored via the appended action plan; this report is provided as an update and overview of the work to date against that plan.

BACKGROUND

The internal data protection audit evaluated all Information Governance processes and policies. As a result, the overall rating was determined to be "Partially Compliant." The Service has been provided with an action plan in order to achieve "Good Assurance".

In collaboration with business areas and the IGB, 28 of the 52 actions have been improved. A data breach in March 2023 has resulted in new actions being added to the plan. The action plan focuses on four main areas of data protection:

1. *Transparency and Accountability:*

    - The IAOs have been provided with a detailed description of their roles and responsibilities, allowing them to perform their duties effectively and enable the SIRO to effectively manage the risks associated with its information assets.

2. *Record Management:*

- The surveillance policy and the data protection policy have been approved by both the IGB and the SLT. The policies will now be consulted with rep bodies and TUs. IGB has approved the Fob policy, but SLT and TUs need to be consulted on them.
- IG is developing a booklet based on the framework to provide guidance to staff and to inform them of the policies and procedures.
- In April the retention schedule was approved by SLT and will be consulted with Rep bodies.
- SLT has reviewed the use of CCTV cameras in various buildings as well as surveillance procedures. It was decided that only three sites would maintain CCTV cameras.
- During the IGB meeting, it was agreed that Property Services would be the IAO for CCTV cameras and fobs. The Surveillance Register will document the locations of each camera, as well as the use of the fob and owners. This approach should be coordinated between the PS and the IG.

3. *Risk and assurance:*

- A variety of aspects of the risk register, including processes, actions, and risks, have been reviewed and improved to ensure that clear control measures are in place.
- As a result of the major data breach, it was highlighted how significant it was to implement a Project Management process. This is to ensure that project closure processes include reviewing all project documentation and data to securely delete any information that is no longer necessary. The action has been completed by I&C and IG.

4. *Training and awareness:*

- Since the Data Protection module was added to the learning platform (learnPro) last year as a mandatory requirement, 1291 people have completed the module, representing 88.1% of the employees.. According to L&D, around 50 people are currently unable to complete the module due to long-term illness, maternity leave, or having recently joined the service/at STC. This is approximately 3% of the workforce.

What is remaining:

- Upon approval of the policies and procedures mentioned above, they should be published on the intranet as well as the ECFRS website.
- Records Management procedures and the methods by which business areas collect, store, and use information should be carefully considered. The DPO has highlighted this point following the major data breach in March. All employees who have access to personal data across the Service, and especially those who are responsible for setting up storage sites or moving files across our digital infrastructure, should have access to permanent guidance regarding ICT storage areas that is secure and appropriate in their storage areas. The service needs to provide clear guidelines and policies regarding who can set up and manage SharePoint Sites and Teams. This will facilitate improved data management and allow informed data storage decisions to be made.

- To prevent further breaches of this nature it is vital that we provide adequate guidance to our staff on this important matter. It is linked to risk number 6 in the legal implications section.
- Ensure that confidential or sensitive information, whether it is documented or discussed, is kept confidential and secure and is not visible to unauthorised individuals.
- Data Protection Awareness: A communication plan and IG booklet is being developed between IG team and DDPO to raise data protection awareness.
- Technical Security documentation must be kept as a living document and reflected in IT policies.
- 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)

OPTIONS AND ANALYSIS

With the implementation of the action plan currently underway, this will assist in reaching the goal of Good Assurance and decreasing the level of organisational risk.

RISKS AND MITIGATIONS

In order to mitigate risks and potential risks, it is important to remain committed to the actions outlined in the plan.

LINKS TO FIRE AND RESCUE PLAN

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

FINANCIAL IMPLICATIONS

ICO fines

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. In addition, we may expose ourselves to risks of claims for compensations for resulting data breaches. 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. An end-to-end procurement process for staff has also been established and approved by the IGB that will be communicated to staff.
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:** Risk have been mitigated. The surveillance policy and procedure document has been approved by the IGB and SLT.

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 after IAOs have completed their asset assessments.
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. A template for information sharing protocols has been established, and the implementation of a data sharing procedure is currently underway.
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. Highlighted on the ICO recommendations. Annex B.
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**: Specific actions have been added to the action plan to ensure compliance with ICO recommendations, however, this risk remains the main concern for ECFRS.
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 on the Service learning platform in May 2022.

STAFFING IMPLICATIONS

The Information Governance team has recruited to the vacancy it was carrying decreasing risk.

EQUALITY AND DIVERSITY IMPLICATIONS

The actions being taken will not have a disproportionate impact on individuals with protected characteristics (as defined within the Equality Act 2010), when compared to all other individuals and will not disadvantage people with protected characteristics.

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

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

HEALTH AND SAFETY IMPLICATIONS

None associated with this paper.

CONSULTATION AND ENGAGEMENT

To include rep bodies, boards, external agencies

FUTURE PLANS

Long term strategic direction

LIST OF BACKGROUND PAPERS AND APPENDICES

Appendix A: Action Plan

Copy%20of%208a%
20Update%20of%20E

Appendix B: ICO Recommendations

Personal%20Data%2
0Security%20Leaflet%