Information Governance Audit Report 2018 - 2019
North Yorkshire Fire and Rescue

For: Executive Board
Status: Final Report
Date Issued: 12th July 2019

1 INTRODUCTION AND SCOPE

Background
In May 2018 the UK adopted the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 18) as its primary data protection legislation replacing the Data Protection Act 1998. This new legislation

- Promotes enforceable accountability,
- Provides greater rights for individuals,
- Recognises the advances of privacy intrusive technology.

One of the biggest changes to the legislation was that for the first time all certain organisations were required to appoint a statutory Data Protection Officer (DPO). The DPO needs to have expert knowledge of information governance legislation and best practice but is also required to be independent from the decision making process within the organisation.

From April 2018 Veritau officially launched its DPO service and provided organisations with a number of resources in order to assist in ensuring compliance with the new tougher Data Protection requirements. This included, amongst other things, a consultancy visit, provision of guidance, and the provision of template documents that could be adopted by the organisation. As part of the service Veritau conducted an Information Governance audit and submitted the findings of that audit in the format of a report which this document fulfils.

2018 – 2019 Priorities
Having recognised that the GDPR and DPA 2018 are very new pieces of legislation, that there has for a long time been a lack of comprehensive information governance guidance for organisations, and that our role as DPO is still very new - our priorities have been to set a foundation of good Data Protection at each of our clients with the intention that going forward we can develop these processes in more detail.

Our first key document to be issued was the GDPR action plan. This set out what steps organisations needed to take in order to achieve compliance with the key data protection principles. This included ensuring that basic documentation, such as Policies and Privacy Notices, had been written and published where required. We also focussed on ensuring key processes, such as Data Breach reporting, had been implemented across the organisation.

2018 – 2019 Audit
As part of the DPO service we undertake an annual Information Governance audit to (a) ensure that key processes have been adequately implemented and (b) to set our main priorities for the next year.

The focus of the audit was to determine whether the organisation has implemented policies and procedures to regulate the processing of personal data and that processing is carried out in accordance with such policies and procedures.

This audit was used to determine potentially high risk areas where the organisation was not compliant, or where lack of action may lead to non-compliance.

The audit was carried out by assessing the organisation's procedures, systems, records and activities, in order to:

- Ensure the appropriate policies and procedures are in place;
- Verify those procedures are being followed;
- Test the adequacy of controls in place;
- Detect breaches or potential breaches in compliance;
- Suggest changes in controls, policy and procedure where appropriate

2019 – 2020 Priorities
Our priorities as DPO for 2019- 2020 have been based upon national trends of non-compliance and where the national regulator has highlighted their own priorities.

This year, with basic Data Protection processes already established in 2018 - 2019, our work will be focussing on the following areas:

- data processing contract management,
- records management,
- information security safeguards,

There will also be a continuing effort to ensure that organisations comply with their Data Protection requirements on a day-to-day basis and that Data Protection is embedded in the organisation's culture.

2 ASSURANCE STATEMENT AND SCORE

Score Awarded: 4 / 5

The score was determined using the answers provided in the questionnaire for the following areas:

- ICO registration
- Adoption of privacy notices and policies
- Updating of employee contract
- Completion of consent forms
- Progress on the information asset register
- Identification of relevant data processors
- Handling of any information security breaches (where applicable)
- Encryption of memory sticks and laptops
- Use of audit trails for electronic systems
- Taking of back ups and ensuring they can be restored if required
- Consent for use of biometrics (where applicable)
- Training

Having completed a site visit and reviewed the organisation's GDPR questionnaire along with accompanying documentation, we are happy with the progress being made. The organisation has robust controls in place to ensure most documentation and processes required by the legislation are in place or will be in place in due course and that Data Protection is beginning to be embedded in the organisation's culture. The organisation still has some work to do in regards to their governance arrangements, information asset register, the use of a destruction log and having a training plan in place (detailed in section 3) but we are confident that this in an ongoing piece of work which will be completed appropriately. It is important to remember that the Information Commissioner has stated that there isn't a deadline for GDPR but that this is a journey of continuous improvement.

3 FINDINGS

GOVERNANCE

The organisation is registered with the Information Commissioner.

The organisation has appointed Simon Dennis as SIRO and Joanne Hawcroft as SPOC. These are appropriately placed people for the roles, and they are aware of their responsibilities having received appropriate training over a period of time. At the time of the audit the organisation advised that the SIRO will soon change to become the Deputy Chief Fire Officer who is an appropriately placed role to carry out this duty. The organisation have confirmed the new individual will be aware of their responsibilities.

The organisation has adopted the following privacy notices and made the relevant people aware of the location and content:

- Staff
- Website
- Recruitment
- CCTV

The organisation also has a number of different service specific privacy notices which have also been reviewed as part of this audit. It has been noted that within the 'Safe and Well' privacy notice the legal basis is not sufficiently clear. Additionally, the organisation should consider as part of their review of their privacy notices the wording used, particularly within the staff privacy notice as it ideally needs to be simplified for easier reading.

All privacy notices are displayed on the organisation's website, however at the time of the audit the 'youth engagement' privacy notice was up for review and therefore was not accessible via the website.

The organisation has adopted the following policies and added them to the policy review cycle:

- Data Protection Policy
- Freedom of Information Environmental Information Regulations Policy
- Freedom of Information Environmental Information Regulations Standard Operating Procedure
- Information Security and Handling Policy
- Information Incident Management Procedure
- ICT User Policy

In addition to the above, the organisation has a Data Subject Rights Request Procedure which is published on the website. It is recommended that this procedure

is updated to include the specific process for internal review as per the legislation. This includes the right to raise any matter with the data protection officer as this is currently not sufficiently clear.

With regards to these policies/procedures there are a number of amendments/considerations which the organisation should now consider which is as follows: The Policies needs to be looked at and reconsidered in relation to their description of the role of the Data Protection Officer as it would appear that these were drafted before the appointment of Veritau. Therefore, certain responsibilities that are allocated to the role are no longer accurate. The Information Security and Handling Policy still appears to be in draft form with comments which needs to be completed and signed off by a suitability senior staff member. The ICT user policy refers to the Data Protection Act 1998 and contains a section about staff members bringing their own devices to work. It is recommended that the paragraph in relation to the staff personal devices in the workplace is reconsidered as in its current format it raises security concerns.

All non-information governance policies have been checked for data protection clauses.

Employee contract templates have been updated to reflect the new Data Protection Act.

Any forms where consent is the legal basis have been updated to ensure they are compliant with the new Data Protection Act.

INFORMATION ASSET REGISTER

The asset register does not contain all the information that we would expect to see. Whilst assets have been listed with asset owners identified who aware of their responsibilities, there are numerous sections which are not included which are required to ensure there is compliance with the specific requirements in relation to the organisation’s processing activities.

The organisation has identified all data processors. Whilst the asset register was not used for this purpose, the organisation did a full review in order to ensure they had captured them all and as such there is a register of data processors. It is of course possible that further data processors will become apparent once the asset register has been completed.

Work has not commenced on reviewing data processing contracts to identify where updated contracts are required.

At the time of the audit, the organisation were entering into new agreements and were working with Veritau to complete the relevant DPIAs.

RETENTION AND DESTRUCTION

The organisation has a detailed retention schedule which was last reviewed and updated in 2018.

There is not a destruction log which includes details of the officer responsible for deletion and/or destruction of the data and when it was carried out currently in operation. This is something the organisation used to utilise and therefore will need to look at reinstating it.

INFORMATION SECURITY

The organisation maintains a log of all information security breaches, and where appropriate has reported the breaches to Veritau.

The organisation uses laptops and these have been encrypted.

All electronic systems are password controlled and have audit trails.

Back ups are taken every night, however due to the quantity of data which is required to be backed up there is a schedule to allow a system of full, incremental or differential back up and it is stored off site. There is also a secondary back up device at a different location. Checks have been carried out to ensure the data can be restored, however, the organisation accepts that further work is required in relation to checks to enable a full assessment of the organisation's capability to restore in the event of an emergency.

Paper records are kept securely, with records being kept in locked cabinets. Additionally, the organisation utilises a securing filing store containing locked cabinets with a signing register for all employees who access the room.

CCTV, BIOMETRICS AND RIPA

The organisation's CCTV system was reviewed on 30th April 2019. This is now forming part of a wider review in relation to surveillance and this has been added by the information governance group to the list of projects needing completion.

The organisation does not use any biometric data.

The organisation is currently reviewing its RIPA policy and has been working with Veritau to complete this. There has however been no RIPA authorisations in the last year.

FOI AND SARs

The organisation regularly receives both FOI and subject access requests and the statistics are reported to and considered by the Information Governance Group. All requests have been logged and 100 percent were answered within the statutory time period.

All staff have been made aware of data protection rights and who to contact if they receive a request. This process was completed by utilising update bulletins, notice boards and staff completing online training modules.

TRAINING

All staff have received basic GDPR awareness training. This was carried out by completing numerous work shops, briefings, staff communications and the completion of online training

Asset owners and SLT have received further training. The training was provided by Aristi, guidance documents were put in the intranet and online modules have been completed.

The organisation does not have a training plan which identifies when all staff are due to receive further data protection training.

The induction pack for new members of staff includes basic data protection instructions. This information is given to temporary and agency staff.

APPENDIX 1 –ACTIONS TO ADDRESS CONTROL WEAKNESSES

	Report Area	Issue	Agreed Action	Priority*	Responsible Officer	Timescale
1	Governance	Update Safe and Well privacy notice to ensure it provides the current legal basis throughout the whole process	Amend privacy notice to include precise information about when consent will be relied upon.	1		
		Wording with privacy notices is not always easy to read	Consider the wording used within the privacy notices to see, where possible, it can be simplified for easier reading	3		
		Youth Engagement Privacy Notice is not available on the website.	Complete review of youth engagement privacy notice to ensure it is published on the website	2		
		Data Subject Rights Request Procedure requirements some amendments.	Update Data Subject Rights Request Procedure to reflect the full process for internal review and the ability to raise any matter with the data protection officer.	1		

		Policies reference to the responsibilities of the Data Protection Officer is not always correct.	Update policies to ensure the role of the Data Protection Officer is sufficiently clear as currently responsibilities are allocated to Vertiau which is incorrect.	1		
		The Information Security and Handling Policy still appears to be in draft form with comments.	Policy to be completed and signed off by a suitability senior staff member.	1		
		The ICT policy refers to the Data Protection Act 1998 and contains a section about staff members bringing their own devices to work which, in its current format raises security concerns.	Legislation to be updated and it is recommended that the paragraph in relation to the staff personal devices in the workplace is reconsidered.	1		
2	Information Asset Register	The asset register does not contain all the information that we would expect to see. Whilst assets have been listed with asset owners identified who aware of their responsibilities, there are numerous sections which are not included	Asset register to be amended to include the following information: • Purpose of processing • Whose personal data does it contain • Types of personal data (including	1		

		which are required to ensure there is compliance with the specific requirements in relation to the organisation's processing activities.	whether there is any special category information), • Retention period, • GDPR Article 6 and 9 basis for sharing • Who the information is shared with (controllor and processor), • Names of third countries or international organisations data is transferred to and safeguards for exceptional transfers of person data to third countries etc if applicable • General description of organisational and technical security measures.			
		Work has not commenced on reviewing data processing contracts to identify where updated contracts are required.	Start reviewing arrangements with all data processors to ensure there is an adequate data processing contract in place.	2		

3	Retention and Destruction	There is not a destruction log which includes details of the officer responsible for deletion and/or destruction of the data and when it was carried out currently in operation.	Organisation need to re-instate destruction log as it is something which used to be used.	1		
4	Information Security	Back up checks are currently not able to occur in a manner which allows for full reassurance that a restore would be possible in the event of an emergency.	Organisation to continue to work on implementing the necessary and agreed suitable provision	2		
5	CCTV, Biometrics and RIPA	Whilst CCTV has been considered, other aspects of surveillance need further consideration.	Commence work in relation to surveillance and make sure there is suitable arrangements in place including but not limited to privacy notices and policy documents.	2		
		RIPA policy review still needs completion	Continue to work towards getting the policy signed off.	2		
6	FOI and SARs					
7	Training	There is currently no training plan in place.	Data Protection to be included within full training plan for the organisation to ensure there is a plan	1		

			for continued training.			

*The priorities for actions are:

Priority 1: Must be carried out as a matter of urgency in order to reduce risk of non-compliance

Priority 2: Should be carried out as soon as possible in order to minimise risk of non-compliance

Priority 3: Requires attention, however low level of risk of non-compliance