Data Protection Action Plan

2021 follow up

Saltney Town Council

December 2021

JDH Business Services Ltd

ACTION PLAN

The priority of the recommendations made is as follows:

Fundamental	Significant	Merits Attention
Action is required to ensure that data protection requirements are not met	Action is required to avoid exposure to significant risk in meeting data protection requirements	Action is advised to enhance personal data controls and security

2021 issue	Categorisation	Accepted (Y/N)	Recommendation	Action taken
Meetings are recorded by the council for the purpose of writing up the minutes, however there is no recording policy in place and the data recordings are not included in the council retention policy/schedule.	Merits attention	Y	*The council should adopt a recording policy for meetings and ensure recordings are included as a data category in the retention policy with a time limit applied for retention of this data*	*Council adopted the recording policy in July 22*

2019/20 issue	Categorisation	Accepted (Y/N)	Action	Recommendation	
A data breach register is not currently used.	Merits Attention	Y	We have provided the council with a best practice data breach register.	*The best practice data breach register should be adopted.* ***2021 follow up – Recommendation Outstanding***	*The Best Practice Data Breach has been adopted July 22*
The town council website is not secured for communication as Hypertext Transfer Protocol Security is not in place (ie HTTPS)	Significant	Y	A HTTPS secured server is required.	*The council should contact the website provider and request the website is moved to HTTPS secured server.* ***2021 follow up – Recommendation Outstanding, however the council website provider has indicated that the current limited usage and functionality of the website does not require HTTPS***	The Clerk will ask the question and find out the costings from Vision ICT it may not warrant the HTTPS

There is no cookie opt in consent available for users of the website There is no website user cookie policy.	Fundamental	Y	The website needs to allow opt in consent to the use of cookies, set optional cookies, and allow user friendly management of cookie settings. A website policy needs to be developed, including the use of cookies.	*The company should work with the website provider to produce a cookies policy and opt in* ***2021 follow up – Implemented***	There is a cookies policy on the website
There is no published third party privacy notice.	Fundamental	Y	We have provided the clerk with a template third party privacy notice, which should be aligned to the council scope and activity, and published on the council website.	*A third party privacy notice should be published on the council website* ***2021 follow up – Recommendation Outstanding***	The Clerk will double check the privacy notice

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up	
The council should compile a data inventory to evidence compliance with the GDPR, in particular:	Significant	Y	Implemented		

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up	
- *the correct lawful basis should be identified for retaining personal data* - *all data subject categories as specified in this report should be included* - *whether or not a data breach should be reported to the ICO for each data subject personal information category if there was a breach*					
The council should adopt an information security policy which also identifies security requirements for members.	Significant	Y	Implemented (Minute ref – Nov 18)		
The council should adopt and adhere strictly to the retention deadlines in a document retention policy. In particular, the council should ensure it is not retaining personal data longer than is necessary to complete the specified purpose(s). *The retention policy should be updated to reflect the data subject categories listed in this report and set time limits for their personal data retention.* *There will need to be time allocated to permanently delete and shred legacy personal data, and other information held in excess of the*	Fundamental	Y	Ongoing implementation – there are currently three boxes of archive information that need to be reviewed with reference to the retention schedule		The Clerk is working through the data a shredding the papers accordingly

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up
time limits set in the newly adopted retention of documents policy. *When a councillor ceases to be a councillor the limits set in the retention policy should be applied to their email history.*				
Data Protection training and cybersecurity awareness training should be provided at induction to employees and members, and on an ongoing basis.	Fundamental	Y	Recommendation outstanding There is also no induction for councillors on data protection/ GDPR and cyber security awareness.	The council should ensure staff and councillors receive data protection training and cybersecurity awareness training. **2021 follow up – Recommendation Outstanding** - the Clerk has received training but councillors have yet to receive specific data protection and cybersecurity awareness training
All archived manual personal information held in excess of the retention deadlines in the document retention policy should be securely shredded	Fundamental	Y	Ongoing implementation – there are currently three boxes of archive information that need to be reviewed with reference to the retention schedule	
Personal information stored on the computer drives should be reviewed by reference to the newly adopted retention policy and data no	Fundamental	Y	Recommendation outstanding. NB the council has reviewed the cost/benefit of using @saltney.gov.uk email addresses	*Personal information stored on the computer drives should be reviewed by reference to the newly adopted retention policy and data no longer required*

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up
longer required should be permanently deleted using only the Permanent Deletion function. *When a member ceases to be a member, the limits set in the retention policy should be applied to the email history of the councilor. This would be very difficult to apply of a non-council email address is used by a member.* *Members should be allocated and only use the* @saltney.gov.uk email address.			but the cost provided by the IT provider was material.	*should be permanently deleted using only the Permanent Deletion function.* *When a member ceases to be a member, the limits set in the retention policy should be applied to the email history of the councillor.* *The council should secure quotations from other providers for the provision of members with @saltney.gov.uk email addresses .* **2021 follow up – Recommendation Outstanding**
The council should discuss with the IT provider the most effective anti-virus software and firewall for the council requirements and ensure it is updated regularly to cover the latest identified cybersecurity threats.	Significant	Y	Implemented	
Photographs should be securely stored until destruction or permanent deletion with all other personal data types. *Photographs should be included in the retention policy and any photographer used will need to comply with the council security requirements.*	Significant	Y	Partially Implemented – photographs held on the computer drives. Limited use of photographs by the council with none used on the website currently containing personal data images	*Photographs should be included in the retention policy and any photographer used will need to comply with the council security requirements.* **2021 follow up – Recommendation Outstanding**

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up
A CCTV code of practice and CCTV policy should be adopted by the council	Significant	Y	Implemented - CCTV cameras are located in the town and only the police have access to the camera drives. Two further CCTV cameras have recently been purchased. No Privacy Impact Assessment has been completed for the surveillance carried out.	*A Surveillance Privacy Impact Assessment should be completed including justification of purpose for the surveillance that is carried out.* **2021 follow up – Recommendation Outstanding**
The Council should ensure appropriate CCTV signage is erected which lists all the purposes the data collected will be used for, as well as providing contact details for the council	Significant	Y	Ongoing implementation - Police are erecting signage as each new camera is installed. New signage is currently being ordered for the older installed cameras	**2021 follow up – Recommendation Outstanding**
Appropriate signage should be used at events so people are fully informed that photos are being taken and are able to opt out if they wish. *If any photographs are taken of minors that, along with other information, can be identified with an individual then the use of these images of minors without guardian consent is a non-compliance under GDPR so clearly appropriate consent is mandatory. The council should identify scenarios where images may be used and*	Fundamental	Y	Implemented – it is council policy to use appropriate signage for events where photographs are taken	

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up
set out clear guidelines to ensure processing is lawful in such situations. *An example approach for non-minor images may be to state within an information security policy that non-identifiable images e.g. group photographs or background photographs, may be used without prior consent (although signage informs people at events that they can opt out). But that any image, when used with associated information, that can uniquely identify an individual, requires written consent before it can be published externally, including on the council website. Once consent has been obtained, the council must ensure they protect the confidentiality of the images until they are permanently deleted in accordance with the retention policy.*				
Appropriate consent will need to be secured (and retained) for enquiries received by letter, email or telephone which relate to third party services eg housing associations, unitary authority and the council needs to forward contact details to a third party	Fundamental	Y	Implemented – it is council policy to seek appropriate consents	
Where the council determines that it is sharing data with relevant third parties and/or third parties are processing council personal data, a	Fundamental	Y	Recommendation outstanding	*Where the council determines that it is sharing data with relevant third parties and/or third parties are processing council personal data, a signed data*

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up
signed data sharing/processing agreement needs to be implemented, and where encryption is required the council should ensure the external provider has implemented this.				*sharing/processing agreement needs to be implemented, and where encryption is required the council should ensure the external provider has implemented this.* **2021 follow up – Recommendation Implemented – agreement signed with payroll agency**
The council should ensure email encryption is available when requited for emailing sensitive personal data.	Significant	Y	Recommendation outstanding - this may be required for communication information to the recently appointed HR/payroll provider	*The council should ensure email encryption is available when required for emailing sensitive personal data.* **2021 follow up – The payroll agency provides access to a password protected portal**
The GDPR requirements for Subject Access Requests which have been adopted by the council should be clearly understood by council staff. Robust template letters should be in place to deal with all key stages of an SAR including securing third party input where required.	Significant	Y	Implemented	
Currently the council is not considering directly delivering new services or projects that would require a Privacy Impact Assessment (PIA) to be carried out. However, the council should adopt a	Significant	Y	*As noted previously a Surveillance Privacy Impact Assessment should be completed including justification of purpose*	**2021 follow up – Recommendation Outstanding**

2018/19 Recommendation	Categorisation	Accepted (Y/N)	2019/20 Follow Up	2019/20 Recommendation and 2021 Follow up
PIA process that utilises a best practice template which will enable a PIA to be carried out effectively if required in the future.			*for the CCTV surveillance that is carried out.*	