

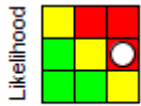
# Cyber Risks and Data Protection Act 2018

Generated on: 14 May 2020



<b>Risk Code</b>	CR62	<b>Risk Title</b>	Cyber Risks
<b>Risk Owner</b>	Howard Crompton	<b>Updated By</b>	Vic Godfrey
<b>Year Identified</b>	2014	<b>Corporate Priority</b>	Be a more welcoming and inclusive council
<b>Risk Description</b>	<p><b>As a result of:</b></p> <ul style="list-style-type: none"> <li>- Computer virus</li> <li>- Malware</li> <li>- Ransomware</li> <li>- Computer hacking</li> <li>- Action by Staff/Member (e.g. opening a malicious link)</li> <li>- Malicious tampering of computer records</li> <li>- Information being sent to the wrong recipient</li> <li>- Loss or damage to server room</li> </ul> <p><b>There is a risk of:</b></p> <ul style="list-style-type: none"> <li>- Systems being interrupted or damaged</li> <li>- Data being corrupted or erased</li> <li>- Personal data being stolen</li> <li>- Breach of the Data Protection Act 2018</li> </ul>		
<b>Opportunities</b>	<ul style="list-style-type: none"> <li>- Safe and effective use of Information Technology</li> </ul>		
<b>Consequences</b>	<p>The consequences of these risks include:</p> <ul style="list-style-type: none"> <li>- Loss of reputation</li> <li>- Ability to provide services is disrupted</li> <li>- Revenue streams are reduced</li> <li>- Additional costs to investigate and test following repair/restoration</li> <li>- Claims for compensation if a third party suffers a financial loss</li> <li>- Fines from the Information Commissioner</li> </ul>		
<b>Work Completed</b>	<ul style="list-style-type: none"> <li>- Information Security policy in place, which applies to staff and Members use of IT systems</li> <li>- Email encryption software (EGress) implemented</li> <li>- Introduced new software (Clearswift and Bloggs) to enhance the checking of threats attempting to attack via the firewall</li> <li>- All data centres have fire suppressing systems and are located in secure areas</li> <li>- Disaster recovery in place at a remote site (Unit 3)</li> <li>- Basic computer insurance provides limited cover for damage to equipment and reinstatement of data (although it does not cover payment of any fines or compensation to third parties)</li> <li>- Business Continuity Plans in place</li> <li>- Ransomware attack resulting in the write-off of IT hardware and infrastructure identified as a financial risk for 2019/20 and 2020/21 (Low/£200k)</li> <li>- Data Protection/FOI SIAS internal audit</li> <li>- Controls in place to ensure any third party providers adhere to NHDC security requirements</li> <li>- Annual PEN Test completed autumn 2018 and PSN Accreditation renewed January 2019</li> <li>- SIAS audit of Cyber Security (March 2018) provided Moderate overall assurance</li> <li>- Implemented specific cyber roles/responsibilities within the ICT team to strengthen resources and approach (September 2018)</li> <li>- Implemented the recommendations from the SIAS audit of Cyber Security</li> <li>- Reviewed findings of the 2018 penetration test and worked through the minor improvements identified</li> <li>- In 2019, the requirement for Members to be registered as Data Controllers with the ICO was removed</li> </ul>		


Cyber Risks and Data Protection Act 2018

	<ul style="list-style-type: none"> <li>- SIAS audit of Cyber Security (August 2019) provided Satisfactory overall assurance and the report made five recommendations (four medium priority and one low priority)</li> <li>- NHDC PSN submission was sent to the Cabinet Office on 19 April 2020</li> </ul>		
<b>Ongoing Work</b>	<ul style="list-style-type: none"> <li>- Anti-virus/malware software in place and automatic updates are performed to servers and all PCs/laptops/tablets</li> <li>- Email Filter monitoring</li> <li>- Web Filter monitoring</li> <li>- Firewalls continually reviewed and updated</li> <li>- Reviewing firewall log files</li> <li>- Microsoft patches kept up to date</li> <li>- Annual PEN Tests to be undertaken and PSN Accreditation to be renewed</li> <li>- Regular advice and reminders issued to users</li> <li>- LMS training available (e.g. annual DPA 2018)</li> <li>- Control/security systems enable potential threats to be identified, investigated and managed accordingly</li> <li>- Regular reminders to all staff and Members are sent by the Service Director - Customers about the need to be vigilant about opening emails from unknown sources</li> <li>- Attending MHCLG Cyber Pathfinder Training Scheme events</li> <li>- Implementing the recommendations from the SIAS audit of Cyber Security (August 2019), including the forthcoming release of a new Cyber Security mandatory training package</li> <li>- NHDC has met and will be inviting an external Cyber Security Specialist in to carry out Cyber Essentials and then Cyber Essentials Plus, which cannot happen until we return to normal day-to-day working and into the offices</li> </ul>		
<b>Current Impact Score</b>	3	<b>Current Likelihood Score</b>	2
<b>Overall Risk Score</b>	8	<b>Current Risk Matrix</b>	
<b>Date Reviewed</b>	21-Apr-2020	<b>Next Review Date</b>	21-Oct-2020
<b>Latest Note</b>	21-Apr-2020 Risk reviewed and updated with Vic Godfrey on 21 April 2020. We need to keep the risk scores as they are, as this continues to be a very highly sensitive area and we cannot get complacent in our approach to managing the associated risks.		

Cyber Risks and Data Protection Act 2018

<b>Risk Code</b>	RR304	<b>Risk Title</b>	Data Protection Act 2018
<b>Risk Owner</b>	Howard Crompton	<b>Updated By</b>	Vic Godfrey
<b>Year Identified</b>	2005	<b>Corporate Priority</b>	
<b>Risk Description</b>	<p>As a result of:</p> <ul style="list-style-type: none"> <li>- Action by individuals (e.g. use of the email system is the predominant cause of breaches)</li> <li>- CCTV systems not being fully compliant</li> <li>- Retention of out of date information on IT systems and in hard copy</li> <li>- Inappropriate use/disclosure of personal information</li> <li>- Fraudulent use of data</li> <li>- Loss or theft of portable devices</li> </ul> <p>There is a risk that:</p> <ul style="list-style-type: none"> <li>- There could be breaches of the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation)</li> </ul>		
<b>Opportunities</b>	<ul style="list-style-type: none"> <li>- Ensuring compliance with legislation and appropriate handling of personal data</li> <li>- Reduced disk storage requirements, leading to reduced costs</li> </ul>		
<b>Consequences</b>	<ul style="list-style-type: none"> <li>- Inappropriate use/disclosure of personal information</li> <li>- Fraudulent use of data</li> <li>- Enforcement/Information Notice being served by the Information Commissioner</li> <li>- Penalties under the General Data Protection Regulation, i.e. 4% of annual global turnover or €20 million, whichever is greater</li> <li>- Loss of reputation and customer confidence/trust</li> </ul>		
<b>Work Completed</b>	<ul style="list-style-type: none"> <li>- Information Security and Internet/Email user policy prevents staff sending emails to their home address</li> <li>- Incident Register in place</li> <li>- Data protection policy in place</li> <li>- NHDC creates its own data sharing protocols on a case-by-case basis; data sharing agreements are in place with all relevant external organisations</li> <li>- Information security policy adopted on the 02 February 2011 and it is reviewed on a regular basis</li> <li>- Purchased Active Navigation software, which highlights duplicate records and out of date information/documentation held on the network and recommends appropriate filing systems for stored information</li> <li>- Egress email encryption software replaced with Clearswift Email Encryption for the corporate wide encrypted and secure sending of personal, confidential and sensitive information outside of the authority</li> <li>- USB encrypted pens are monitored by GIF Software</li> <li>- All NHDC CCTV systems are fully data compliant</li> <li>- ICT has ownership of all CCTV devices within the authority buildings, which also includes displayed signage and extraction of data when requested via a Subject Access Request (SAR)</li> <li>- Software in place to redact images if there is a request for CCTV images (the amount of time required to redact images manually was lengthy/costly)</li> <li>- Network log-in screens detail terms/conditions of use</li> <li>- NHDC data protected on portable devices</li> <li>- Financial risk identified for 2020/21: <ul style="list-style-type: none"> <li>-- Fines for breaches of the EU General Data Protection Regulation by the Council or by NHDC outsourced providers when handling and storing data originally collected by NHDC (Low/£500K)</li> </ul> </li> <li>- SIAS audit of Data Protection and Freedom of Information (December 2016) provided moderate overall assurance</li> <li>- Officer seconded to the Information Team to help with preparations for the General Data Protection Regulation</li> <li>- Auto-forwarding of emails was switched off on 26 June 2017, in line with the high priority SIAS audit recommendation</li> <li>- Presentation to Senior Managers Group (November 2017)</li> <li>- Implemented the recommendations from the SIAS audit of Data Protection and Freedom of Information (December 2016)</li> </ul>		

Cyber Risks and Data Protection Act 2018

	<ul style="list-style-type: none"> <li>- Full information audit completed, including gap analysis and review of processes/procedures, and agreed actions implemented to ensure compliance with the General Data Protection Regulation</li> <li>- Member information/training sessions</li> <li>- SIAS audit of General Data Protection Regulations (July 2018) provided Satisfactory overall assurance</li> <li>- Designated Data Protection Officer in place</li> <li>- Information Security Policy published</li> <li>- Developed strategy for officers/Members to use BlackBerry Apps to deliver better services at reduced cost across the authority</li> <li>- Completed required changes to documentation, e.g. fair processing notices</li> <li>- Implemented the recommendations from the SIAS audit of General Data Protection Regulations (July 2018)</li> <li>- Requirement for Members to register as a Data Controller with the ICO removed in 2019 (previously, if requested by Members, officers did this on their behalf, including payment of the fee)</li> <li>- GDPR Operational SIAS audit report received in October 2019 provided Satisfactory overall assurance (two medium and two low priority recommendations)</li> </ul>		
<b>Ongoing Work</b>	<ul style="list-style-type: none"> <li>- Mandatory annual training via e-learning; completion by staff monitored and escalation processes in place</li> <li>- Regular reminders to staff and Members on the use of email</li> <li>- The use of email quotas forces individuals to review the data they are keeping</li> <li>- Continue to implement/monitor the Active Navigation tool</li> <li>- Information Team works with service areas to ensure all departments are keeping documents in line with their retention schedules</li> <li>- Annual review of CCTV in Operation notices to ensure they are up to date and fully displayed (all areas covered by cameras, including meeting rooms)</li> <li>- Monthly tests of all CCTV data extraction processes are carried out</li> <li>- ICT control and monitor regularly data storage and retention in off site facility</li> <li>- Identified DPA breaches reported to the ICO if required; so far, the ICO has not instigated any formal action</li> <li>- Ongoing communication with officers and Members to raise awareness</li> <li>- Regular officer meetings to review/discuss DPA 2018 issues</li> <li>- Implementation of new systems/databases require the completion of Privacy Impact Assessments and if required, Data Processing Agreements</li> </ul>		
<b>Current Impact Score</b>	2	<b>Current Likelihood Score</b>	2
<b>Overall Risk Score</b>	5	<b>Current Risk Matrix</b>	
<b>Date Reviewed</b>	21-Apr-2020	<b>Next Review Date</b>	21-Oct-2020
<b>Latest Note</b>	<p>22-Apr-2020 Risk reviewed with Vic Godfrey on 21 April 2020. The Information Compliance Team continue to work with the L&amp;D Team to review the LMS to ensure colleagues are completing the Essential Data Protection Training. Impact score reduced from High to Medium, in view of the likely value of any ICO penalty and the mitigating measures we have in place, although it is acknowledged that the impact would also be reputational, which could be significant for the Council. The reduced overall risk score of 5 is a fairer reflection of the current risks to the Council.</p>		