ADUR & WORTHING
COUNCILS

Joint Strategic Committee
6 June 2017
Agenda Item 6

Ward: [All]

Staying Secure in a Digital World

Report by the Director for Digital & Resources

1.0 Summary

1.1 The purpose of this report is to provide committee with an update on the cybersecurity arrangements that are in place keep the Councils' networks, computer system and information assets safe and secure. As we move forward with our digital technology strategy (see the Joint Strategic Committee report, 2nd Dec 2014), increasingly moving to cloud-based services, it is crucial to keep our approach to cybersecurity updated, while ensuring that our existing network infrastructure is protected.

1.2 The Data Protection Act 1998 (DPA) requires that Data Controller (the Council) complies with the principles within, including to have security measures in place to protect personal data. In May 2018 the General Data Protection Regulation (GDPR) comes into force and supersedes the DPA. The most significant addition in the GDPR is the accountability principle : the Controller (the Council) shall be responsible for, and be able to demonstrate compliance with the GDPR principles. This report contributes to the Council demonstrating how it protects personal data.

1.3 Information security is of paramount importance to our organisation, and whilst this report was commissioned well before the recent attack affecting the NHS, it is a timely statement of our approach to security and our ongoing efforts to continuously improve our position.

2.0 Background

2.2 Cybersecurity covers the protection of computers, networks, programs and data from unauthorized access or denial of service. Maintaining security is not just the remit of the ICT department as security responsibilities extend to all staff, Councillors, contractors and our suppliers.

2.1 Modern organisations now demand effective, efficient digital services available from anywhere, from a wide range of devices. Enabling the business securely is a critical requirement in our digital age. Our strategy to adopt cloud technologies is beneficial to our security arrangements. The leading platform and infrastructure technology companies we use are continually developing their approaches to cyber-security in the face of ongoing threats and have the resources and expertise to deliver the highest levels of security. Adur & Worthing Councils have taken the right strategic decisions to adopt these technologies -

ones that provide the benefits of digital service delivery with the most advanced cybersecurity.

2.2 Our new software platforms Google, Salesforce and Matssoft are highly secured by industry leading security teams, with our current on-premise applications soon to be recipients of this care and attention, as we move to leading cloud datacentre providers Microsoft Azure and Amazon Web Services (see the Joint Strategic Committee report, 13 July 2016 - Moving to the cloud).

2.3 An example of a common type of cyber threat and the Councils readniess was the malware attack, WannaCrypt on 12th May 2017

2.3.1 The world wide 'Ransomware[1]' attack, struck c150,000 organisations in 150 countries including sections within the NHS. The ransomware, known as WannaCrypt encrypted the contents of computer hard drives, preventing users from accessing their data and services whilst demanding a ransom to be paid.

2.3.2 As a result of the Council's IT security systems being routinely maintained and updated, there was no compromise to any of the council's systems, data or devices. All Council Services continued to run without disruption.

2.3.3 The Councils' ICT and Digital and Emergency planning staff reviewed and confirmed the status of system security. This review identified several areas of low-lying risk to be addressed and took appropriate remedial steps.

2.3.4 Council Staff and managers were kept informed throughout the period and were reminded to be diligent with regard their part to play in reducing the risk, for example they were reminded not to open any unsolicited email, nor click through any internet link where the source can not be identified and trusted.

3.0 Adur & Worthing's Architecture and Solutions

3.1 The connected nature of the Councils' ICT infrastructure and arrangements enables staff to access computer systems through a blend of on site and cloud hosted services, providing them with the same experience in the both the council office and home office.

Cloud Services

3.2 Secure cloud-based services are now crucial to the way commercial and government services are delivered to customers, business-to-business and to staff. Due to the constantly changing nature of technology and emerging threats there is a need to continually assess and validate the security arrangements in place by the cloud services we use and we follow the guidance on such services published by the National Cyber Security Centre.

3.3 Cloud vendors continually invest in improving the security architecture of their products. The wide range of their customers mandate certain levels of assurance, which are often higher

[1] Malware, short for malicious software, (also known as computer viruses) is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems. Ransomware refers to the type of malware that carries out an extortion attack that blocks access to data until a ransom is paid.

that the standard set by local government. International standards ISO 27001, ISO 27017 & ISO 27018 as well as CSA * certifications are held by the cloud providers that we will be engaging with. The council is responsible for ensuring that the data hosted is secured in an appropriate manner.

Local Network & Devices

3.4 It is not by chance or luck that the Council has not been affected by a cyber attack. The following is a summary of the ways that cybersecurity has been applied across the Council.

3.5 Several layers of managed firewalls prevent unauthorised external access of the internal network. Where external inbound connections are required by business need, the scope and nature of the connection is tightly governed by predefined rules. Fully documented, peer reviewed change requests are required to amend these rules. Where possible the connection is encrypted to ensure integrity of the data transferred, and prevent attacks such as 'Man-in-the-Middle'.

3.6 Authenticated web proxy, servers, mobile device management (MDM), storage encryption, backup encryption, device control policies, anti-malware and software deployment products ensure that devices and media used for storing and accessing Council data are protected from malicious code and other threats. The council deploys a wide range of industry standard products such as Forcepoint Web Security, Lumension Endpoint Security, Microsoft Group Policy, Bitlocker, System Center Configuration Manager, and GFI Languard.

3.7 Access control systems define who has access to what resources when. This relies on a system called Active Directory, an industry standard user directory system built on the foundation of highly-available and reliable infrastructure.

3.8 Proactive monitoring of key operational systems ensure problems are known to ICT operations staff, and remedial action can be taken in advance of an incident occurring. Unusual activity on the network is logged and brought to the attention of senior 3rd Line Technicians, data that can be indicative of an attack but also invaluable for capacity planning. *Cisco Prime Infrastructure* is in the process of being installed, which will allow centralised monitoring, patching and maintenance of core network infrastructure including Wi-Fi access points.

3.9 As referenced in the section about the Council's PSN code of connection, the datacentre and internal network is subject to an annual health check and penetration test. The output of this test forms the basis of a remedial plan, the progress of which is reviewed monthly by the IT Service Operations Team Leader. This is part of the purview of the Security Operations Group which reviews security threats and implications at a highly technical level.

3.10 Requests for access to both cloud services and the internal network (new starters, contractor access) are processed through a new starters process where requests are documented and require management approval. Leaver requests are similarly processed and form part of the HR processes to terminating employment. This means that no staff leaver accounts shall remain active following their departure date.

3.11 Automated Microsoft Windows patching processes ensure the latest software update on on staff devices, so staff are protected from malware, known vulnerabilities resulting from out-of-date software. ICT operations staff maintain an overview on NCSC, industry message boards and vendor information bulletins to ensure vulnerabilities are mitigated as soon as possible.

3.12 The Council's public Wi-Fi service is cryptographically separated from the Council's internal network and computer systems within that protection. The council's internal Wi-Fi service is only available to staff with an authenticated Council device.

3.13 Access to the Council secure internal network and services is permitted only on Council provided laptops and personal computers.

3.14 Council provided iPads, tablets and smartphones are fully encrypted to AES256 standard and are only permitted to connect to the public WiFi service, as such they have no access to the secure internal network.

3.15 In addition to encryption services,all Council smartphones have Google security and device management controls installed and configured enabling them to be wiped, this may be performed on a specific Google account or the whole phone.

3.16 The Council has a Bring Your Own Device (BYOD) provision that allows staff members to access email and cloud-based productivity services from any device . The corporate telephone system, cloud hosted systems and applications on the Council Digital Platform are also available from BYOD devices by virtue of the services being made securely accessible via internet connectivity and secure logons. Services exclusively hosted from the Council's network are not accessible to BYOD devices.

Key technology platforms

3.17 Our website, www.adur-worthing.gov.uk is hosted on site currently, and is primarily protected within the Council's network security web server arrangements (see section 7.1). In addition, the site uses the gold standard for web site security: https:// protocols (the ‘s’ in https:// = secure). This encrypts all communications between the website and user. These arrangements together with close monitoring and security reviews thwart any cyber attacks to attack or take over the web site. There are 12 micro web sites e.g www.itjunction.org.uk, that the council hosts using Wordpress. Security updates, monitoring and patches are kept uptodate thwarting frequent attacks and hacking attempts.

3.18 Matsoft and Salesforce platforms together form the Council’s (Cloud) Digital platform, and an increasing number of council internal and customer facing services are built and hosted on these solutions. The responsibility for cybersecurity for these services rests with both the platform suppliers and the Council. The following independent security assurance work has been undertaken by certified security consultants.

- Risk based approach to information classification and information security management - Aug 2015

- Risk assessment of the Digital platform - Nov 2016
- Mazars audit of the Digital platform - Nov 2016
- Assessment of Matsoft PEN test and audit of the council's Digital platform configuration settings - Apr 2017.

The Council's Matsoft data is hosted on Amazon Web Services (AWS). AWS have highly compliant security certifications, assertion and operates a highly secure and reliable cloud infrastructures, and is used by other leading councils such as Peterborough, Aylesbury and Bristol, as well as a host of central government departments including the Ministry of Justice.

Google Suite (Email, Calendar, Gdrive, Hangouts)

3.19 Google has a highly compliant security certifications, assertion and operates a highly secure and reliable cloud infrastructures.

- Google cloud infrastructure protects data 24/7 : From custom-designed data centres to undersea fibre cables that transfer data between continents, . Data is distributed across multiple data centers, so that in the event of a fire or disaster, it can be automatically and seamlessly shifted to stable and secure locations.

- Encryption keeps data private while in transit : When you do things like send an email, share a video, visit a website or store photos, the data that is create moves between your device and Google data centres. This is protected by multiple layers of security, including leading encryption technology like HTTPS and Transport Layer Security.

- Threat detection helps protect Google services : Google continuously monitor its services and underlying infrastructure to protect them from threats, including spam, malware, viruses and other forms of malicious code.

- Gmail encryption keeps emails private : Gmail has supported encrypted connections, which makes it harder for hackers to read emails. Gmail also warns users about possible security risks, like when you receive an email that was not sent over an encrypted connection.

- Gmail spam protection filters out suspicious emails : Many malware and phishing attacks start with an email. Gmail security protects users from spam, phishing and malware. Gmail analyses patterns drawn from billions of messages to identify characteristics of emails that users marked as spam, then uses those markers to block suspicious or dangerous emails before they ever reach users. Users can help by selecting "Report Spam" for suspicious emails. Machine learning and artificial intelligence enable Gmail's spam filter become ever-more accurate.

- Chrome automatically updates your browser security : Security technologies are always changing, so staying safe means staying up to date. The Chrome browser automatically checks regularly to make sure that the version of the browser being used is updated with the latest security fixes, protections from malware and deceptive sites.

- Google Play keeps potentially harmful apps off smartphones : One of a device's biggest security vulnerabilities can be the apps installed on it. Google's detection system flags potentially harmful apps before they ever reach the Play Store.

- Security rewards programmes : Google have a security rewards programmes that pay independent researchers to find vulnerabilities in their services and create security fixes.

7.8.2 The Council has control over its own Google configurable features and settings that can be invoked to enhance security and data management practices. The CESG Google Apps security guidance has been used to inform the Council's setting, such as :

- Enforcing strong passwords
- Enforcing 2 factor login authentication
- Enforcing email encryption
- Enforced mobile device management
- Enforce mobile phone encryption, pin and screen lock.
- Remote wipe of an email account.

An annual independent security assessment check is undertaken on the Council's Google domain configuration in liaison with Google and the Councils Google deployment partner. The Security Operations Group monitor and progress actions from the security assessment.

Council staff can take control and undertake their own checks on their Google Apps account :

- Secure your account with the Security Checkup
- Privacy check
- Get alerts about suspicious activity
- Strengthen sign-in to prevent attacks
- Safeguarding Google account if the event of losing a phone.

  Staff have access to training resources and can run their own privacy and security checks on their accounts.

4.0 Council's Governance arrangements

4.1 Cybersecurity is not just about technical controls of course, but relies on our staff understanding the importance of protecting information appropriately. Good governance and information management is required from end-to-end, implemented in a way that is safe but does not restrict or constrain the business unnecessarily. It is vital that our Council's information assets are safe and secure while at the same time having proportionate and appropriate security controls and policies. There are many ways we secure and reduce risks, by using:

- Physical controls like walls, locked doors and door access management management
- Procedural controls like making managers responsible for access, audits, allocation and retrieval of devices, ensuring staff hold appropriate systems access (using the principle of least privilege).
- Regulatory controls in policy and contract conditions
- Adherence to industry standards, codes of practice and government guidelines
- Undertaking risk assessments and identifying continuous improvements
- Mandating staff security training and raising awareness on social engineering and common attack methods (phishing emails, CEO fraud and other spoofing attacks)
- Technical controls like cryptographic software, authentication and authorisation systems or secure protocols, penetration testing
- Security and legal professional advice and support
- Disaster recovery and business continuity planning and testing

The Council has a suite of information security policies. The policies sets out the approach of the Council regarding the security of our information assets to guarantee the confidentiality, integrity and availability of Council information and systems. At present, the policy suite is being reviewed and updated by an independent security consultant commissioned by the Census partnership. The policies define roles in the organisation with responsibility for information security which are strongly established at Adur & Worthing.

4.2 Included in staff T&Cs and employee handbook are acceptable use, email and internet policies. Staff have to complete an information security e-learning module when first in post and then 3 yearly (a review is pending on changing this to annually). Additional and up to date guidance and advice is published on the intranet, including: Bring your own device, setting up smartphones, working abroad, device guardianship, Social engineering and fake emails (phishing).

Updates and alerts are communicated to staff via email and through intranet communications channels. If in doubt on a matter of data security staff are encouraged and signposted to contact the ICT helpdesk, the Information security manager or Data Protection Officer for advice and support.

A key part of the Council cybersecurity is for all staff, Councillors and contractors to have good information security practices, including phishing attacks. We all like to think we can spot one, but the fraudsters are very clever in fooling us to divulge information which can then be used to obtain personal, financial information. Staff are signposted to guides to help raise their awareness.

The Information security e-learning module is due to be reviewed and updated, including making it mandatory to undertake the module annually.

4.3 The Senior information Risk Owner (Paul Brewer, Director of Digital and Resource) is accountable for :

a. Informing the Chief Executive of all current developments in security practices and monitor the revision of the Information Security Policy Suite and any supporting standards, guidelines and procedures as required;
b. Delegating as required the authority to monitor compliance with the Information Security Policy Suite to such officer(s) as deemed fit to discharge such a function, e.g.

Information Security Manager;

c. Ensuring that information governance is embedded into the organisation;
d. Ensuring that potential risks to corporate information are mitigated;
e. Ensuring that resources are available to provide such protective measures as may be appropriate to meet security requirements, e.g. finance, people, etc.

4.4 Unlike many councils, we have chosen to maintain a dedicated post to ensure our standards are maintained and improved. The Information Security Manager (Barbara Bastable) is responsible for :

a. Developing, monitoring and overseeing the implementation of the Information Security Policy Suite and any associated standards, guidelines and procedures;
b. Ensuring that all staff and Members are aware of the information security policies, standards, guidelines and procedures and where necessary ensure that the Council provides instruction and training in security matters;
c. Providing advice and support to Information Asset Owners
d. Providing advice and support to Digital/ICT, groups, SIRO, Councillors and staff.
e. Review teh security arragnments and ation for the Councils key Digital platforms.

4.5 The ICT Operations Manager (Simon Taylor) is responsible for :

a. Regularly reviewing security measures in place at Adur and Worthing Council's Data Centre, Desktop Client environment and networks (local physical and WAN links).
b. Facilitating operational ICT resources participation in IT health checks (Pen Tests), PSN reassessment, audits and investigations and ensuring the remediation or mitigation of any identified risks or issues.
c. Providing reports on the state of Adur and Worthing Council's security patching for Servers, PCs (inc Laptops) and Network switches.
d. Chairing the Monthly 'Security Operations Group' Meetings
e. Coordinating the incident management response for ICT Major Incidents affecting the Council's ICT environment.
f. Reporting any identified deficiencies in staff, councillor, contractor, or supplier behaviour presenting a risk to the ongoing security of the Council's data systems.

4.6 The Digital Programme Board, Digital Operations Group and Security Operations Group have responsibilities for strategic and operational security arrangements . See Appendix A.

5.0 Audit regimes

5.1 There is a robust, stringent and continual audit regime of the Council's security policies, controls and arrangements across the whole scope of Digital and ICT services provided in-house and by suppliers. Recommendations from the audits are actively monitored and actioned.

Internal Audits, undertaken by Mazars (from 2013):

- IT Project Management & Governance (CenSus Contract) - June 13
- IT Asset Management – Oct 13

- Data Centre – Nov 13
- Joint Website – Nov 13
- Delivery of Digital Strategy – Feb 17
- ICT Helpdesk - Mar 2014
- ICT Network Infrastructure - Apr 2014
- FOI Audit - 2014

- Data Protection and Information Governance - Mar 2015
- Disaster Recovery - July 2015
- Public Service Network - Sept 2015
- ITIL Service desk - Sept 2015
- Cloud Computing - Nov 2016
- Google Implementaion - Jan 2017
- Remote access - April 2017
- IT resilience - April 2017
- Telecom contract - April 2017
- Mobile phone contract - in progress

The 17/18 plan includes the following audits:-

- Compliance with the new General Data Protection Regulations
- ICT Management & Strategy
- Cyber Security
- Thematic review of password security of all key system
- Web Security
- Mobile Devices

Public Services Network Audit

5.2 The PSN is the government's secure, high-performance network. For the Council to have a connection to the PSN, it must pass a successful code of connection (CoCo) submission annually. The council has successfully passed the CoCo every year.

The process of completing a CoCo submission includes an independent IT health check (ITHC), providing internal and external penetration testing (Pen testing). Pen testing is a process whereby certified IT security consultants attempt to gain access to Council Systems using ethical hacking software methods. Key areas covered in ITHC are :

- Boundary firewalls [to prevent unauthorised access]
- Secure configuration [setting up systems securely]
- User Access control [restricting access to those who need it]
- Malware protection [i.e. using anti-virus software]
- Patch management [i.e. updating software]

Passing the PSN submission and achieving accreditation means that we are able to connect to secure resources across the PSN, such as protected systems hosted by the Department of Work and Pensions. The ITHC also forms the basis of a remediation action

plan to improve security across the Council's internal network, providing valuable insight into how the internal technical controls the Council deploys measure against industry and NCSC best practice. The remediation plan prioritises remediation of risks by their threat severity level.

Adur and Worthing have a good track record remediation of identified risks promptly following receipt of the health check reports.

6.0 Standards and good practice

The publications, guidance and advice from the NCSC and GDS informs the Council's Digital programme and cybersecurity policies, controls and arrangements.

6.1 National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) is the UK Government's authority on cyber security. The NCSC brings together and replaces CESG (the former information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

The NCSC's main purpose is to reduce the cyber security risk to the UK by improving its cybersecurity and cyber resilience. They work together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management

6.2 Government Digital Services

The Government Digital Services (GDS) is part of the Cabinet Office and the Efficiency and Reform Group. They are responsible for :

- Provide best practice guidance and advice for consistent, coherent, high quality services
- Identify the needs for common services, components and tools, building some ourselves and helping departments build others
- Run model projects with government and other partners to show what's possible
- Help government choose the right technology, favouring shorter, more flexible relationships with a wider variety of suppliers
- Set and enforce standards for digital services
- Lead the Digital, Data and Technology function for government

7.0 Migration of on-site hosted computer systems to the cloud

7.1 The CenSus ICT Partnership teams (A&W, Mid Sussex and Horsham) are running a project to migrate Council services hosted locally, within local secure local data centres, to secure public cloud computing hosts. In simple terms this is moving applications hosted in our on-site data centre at the Town Hall to secure off-site data centres within the UK, hosted by Amazon Web Services (AWS) and Microsoft Azure. Both have highly compliant security certifications, assertion and operate highly secured and reliable cloud infrastructures.

7.2 Plans are progressing to commission a Managed Service Provider (MSP) to work alongside the CenSus ICT partners in creating a cloud infrastructure design that is secure and compliant with all appropriate standards. The MSP will assist the councils in migrating the infrastructure to the cloud, whilst ensuring there is no impact to the business. The selected MSP was chosen on the basis of their skills and experiences in undertaking a similar migrations for other organisations in the public sector including. They will work closely with Councils Digital / ICT officers to ensure appropriately robust, security measures are applied in-line with current best practice (noting also that regular review and penetration testing will also be performed to confirm the integrity of security measures).

7.3 The chosen cloud providers have shown that they are compliant with the current security standards that are required to host local government infrastructure. Due to the focus on cloud security, cloud vendors are investing significant sums of money to ensure that cloud security is as good if not better than local government resources can provide. ISO 27001, ISO 27017 & ISO 27018 as well as CSA* certifications are held by the cloud providers that we will be engaging with. The council will be responsible for ensuring that the data hosted is secured in an appropriate manner.

8.0 Disaster Recovery

8.1 In order to ensure that Council Services can be restored in the event of an emergency, IT Services have a disaster recovery plan outlining the actions to be taken in a loss of one or more services.

The council has a number of key resilience measures in place already to mitigate for loss of service. These include:

- Email and Telephony Services hosted in the Cloud
- Front line and business continuity management services hosted on Salesforce and Matsoft platforms hosted in the cloud.
- Locally held data is backed up to disk locally and remotely (Horsham DC's Data Centre), encrypted tape backups held elsewhere within the district (2.5 miles from Worthing Data Centre).
- Uninterruptable Power Supplies within the Data Centres and Comms Rooms
- Contract for Emergency Generator Power Supply in place

Most commonly, service interrupting incidents are managed locally through our standard IT incident management processes (covers day to day service or technical failures).

In preparation of this the Council's Emergency Planning Officer has worked extensively over the last year on a process of creating a corporate Business Impact Assessment (BIA), which identifies all of the Council's key services and the risk that a loss of service poses to the organisation and those reliant on it. From this work a new Business Continuity Plan is being developed. This plan essentially deals with loss of buildings, staff, equipment and suppliers. There is an ICT risk element to the Business Impact Analysis which asks staff to

consider what steps can be taken to mitigate from an ICT failure. This predominately uses manual processing and procedures.

The data collected through this process enables the organisation to direct business continuity and disaster recovery efforts.

Digital, CenSus ICT and Business Services (including surveyors, facilities management and emergency planning) are jointly undertaking a disaster recovery test in late summer / early autumn 2017. This test is designed to simulate a significant service impacting incident, resulting in the loss of all on-site IT infrastructure services. A separate progress report is being produced for the June Joint Governance Committee.

8.0 Legal

8.1 The Council must comply with the Data Protection Act 1998 and the principles within, including:

> Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8.2 The General Data Protection Regulations comes into force May 2018 and supersedes the Data Protection Act 1998. The Council must comply with the Principles within, including:

> Article 5, Principle 1(f) Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using appropriate technical or organisational measures.
>
> Article 5, Principle 2 The Controller (Adur & Worthing Councils) shall be responsible for, and be able to demonstrate compliance with principle 1(a) - (f).

9.0 Financial implications

9.1 Cybersecurity is covered within exisiting budgets

10.0 Recommendation

10.1 Joint Strategic Committee is recommended:

i) Note the contents of this report

Local Government Act 1972
Background Papers:

2nd Dec 2014, Joint Strategic Committee, Investing in new technology : The springboard to excellent customer experience and business efficiency

12th Dec 2014, CenSus (Central Sussex Partnership) Joint Committee : Adur & Worthing Digital Strategy Update

13th July 2016, Joint Strategic Committee, Moving to the cloud

Contact Officer:

Barbara Bastable
Senior Information Officer
01903 221007
barbara.bastable@adur-worthing.gov.uk

Schedule of Other Matters

1.0 Council Priority

1.1 Services and solutions are increasingly being made available by digital means, placing requirements on us as an organisation to enable business change flexibly but securely. Developing our technology platforms and increasing access from anywhere is essential for our ongoing transformation, but must be tackled in a way that ensures the security of our citizen's information.

2.0 Specific Action Plans

2.1 The work is developed and managed as part of our Digital Programme

3.0 Sustainability Issues

3.1 Our key provider of cloud services, Amazon Web Services has a long term commitment to achieve 100% energy usage from renewables, with a target of 50% for 2017.

4.0 Equality Issues

4.1 Matter considered and no issues identified

5.0 Community Safety Issues (Section 17)

5.1 Matter considered and no issues identified

6.0 Human Rights Issues

6.1 Privacy and security issues are the most important issues for citizens in relation to government use of ICT, particularly data, and it will be essential to strike the balance of risk and reward here, and communicate exceptionally well with residents and members.

7.0 Reputation

7.1 ICT failure has a considerable impact on the Councils' ability to deliver services and thus on our reputation. One of the core objectives of this project is to reduce the likelihood and impact of ICT failure.

7.2 The Councils have achieved a good national reputation for innovation in ICT and digital. Good and continual cyber security will help to continue that.

8.0 Consultations

8.1 Matter considered and no issues identified

9.0 Risk Assessment

9.1 The Councils currently have risks identified around the lack of reliable ICT infrastructure and disaster recovery and intend to keep these high on the agenda. These are managed through the service risk and corporate risk management processes.

10.0 Health & Safety Issues

10.1 Matter considered and no issues identified

11.0 Procurement Strategy

11.1 Matter considered and no issues identified

12.0 Partnership Working

12.1 The Councils are engaged with our partners in CenSus ICT.

Appendix A - Governance arrangements

Digital Programme Board

The Digital Programme Board is part of overall strategic governance for the councils, reporting to the Change Board. It aims to drive the development of truly user-centred digital services across the organisation, and continuously improve core ICT delivery.

- Minuted monthly, charied by the Director of Digital & Resources.
- Develop “design & change practice” to ensure all work is user-centred
- Develop and manage a prioritised programme to 1) create efficient, user-centred digital services people choose to use and 2) deliver business critical ICT change, improvement & service delivery
- Migrate services on to the Salesforce/MATS platform as a default choice, with open standards compliant applications a possible alternative
- Control digital/ICT spend, including improved contract and supplier management
- Ensure effective and proportionate information governance & security
- Develop the digital/ICT operating model, including modernising the CenSus partnership
- Horizon scan, developing technology strategy to stay ahead
- Deliver engaging and informative internal and external communications

Digital Operations Group

- Minuted weekly ICT and Digital Operational Management group meeting chaired by the Head of Digital
- Monitor progress of ongoing service provision within the sphere of business as usual (day to day).
- Reviews submissions from the business to improve services through the use of technology
- Reviews service support operation of internal and external suppliers - seeking remediation for service performance issues wherever they arise.
- Identifies and reviews opportunities for continual service improvement through trend review and problem identification and management

Security Operations Group

- Minuted monthly service management and technical operations review focussed entirely around security provision chaired by the Head of Digital.
- Review Remediation Action Plan (RAP) from ITHC reports, internal audits and incidents/problems.
- Review existing security measures pertaining Council services wherever they are hosted.
- Review security related incidents arising in the period since the last meeting.
- Review of monthly security patching reports and backup recovery reports.
- Discuss security related change requirements (enhancements or implementing changes in response to changing security advice from HMG or other governing bodies).
- Monitoring and review of Digital platform and Google security assurance.