Joint Governance Committee
27 September 2022

ADUR & WORTHING
COUNCILS

Ward(s) Affected: All

Response to IT audit findings and update

Report by the Director for Digital, Sustainability and Resources

Officer Contact Details
Paul Brewer, Director for Digital, Sustainability & Resources
07881 323 471, paul.brewer@adur-worthing.gov.uk

Executive Summary

1. Purpose

1.1. This report has been produced as a response to concerns raised by the Joint Governance Committee in relation to IT and information governance/data protection services at the Councils.

1.2. It follows the presentation by the internal audit team at the committee meeting on 28th July 2022 which provided an overview of 4 internal audits relating to those services.

1.3. The report provides additional information, context and updates to provide a fuller and more up to date picture of the arrangements in place and the progress made since audits were completed.

1.4. The report will be presented by Paul Brewer, Director for Digital, Sustainability & Resources.

2. Recommendations

2.1. That Joint Governance Committee notes the contents of the report.

3. Context

3.1. On the 28th July 2022, Joint Governance Committee received a presentation from the internal auditor regarding the outcomes of four internal IT and information governance related audits.

3.2. The four audits were as follows

- Data protection (planning and development service) - limited
- Disaster recovery - limited
- Cybersecurity - satisfactory
- Cloud computing (draft) - satisfactory

3.3. The Committee requested that the Director for Digital, Sustainability & Resources attend the next Joint Governance Committee to provide further explanation and present plans for improvement.

3.4. This report has been produced by the Director and wider team in advance in order to provide a detailed update and enable a more fully informed discussion at the committee meeting.

4. Issues for consideration

4.1. The provision of secure and reliable IT systems is a critical requirement for the effective and safe functioning of any organisation in the modern age.

4.2. Beyond the important technical considerations, members of the committee have rightly highlighted the crucial role of human users in ensuring a secure and safe system overall, particularly when it comes to the appropriate and secure handling of data and access to systems.

4.3. This report seeks to provide additional information to inform the committee of the current position, provide progress made since audits were undertaken, while recognising there is important improvement

work still to be done.

4.4. Much of the discussion in the committee meeting on 28th July was with regard to the two areas with limited assurance, data protection and disaster recovery. The report seeks to respond to those, while also providing further information on cyber and cloud computing.

4.5. It is important to note that leadership in the digital function is in transition. As part of the organisational design work being led by the Chief Executive, our current Head Customer Services & Digital is now also Head of Waste & Cleansing, and with the industrial dispute in recent months, there has been very significant workload there, which continues. We are very grateful to Jan Jonker, who has done an extremely good job.

4.6. This has not affected the good work by managers in digital to continually improve the service, but it has meant that the “bringing together” of the work, in the way presented in this report, has been more difficult to achieve. Paul Brewer, Director, is now playing a more active role in this interim phase, to ensure that appropriate leadership focus can also be maintained in Waste.

4.7. With regard to overall governance of IT, digital and data, the Director for Digital, Sustainability & Resources is the Senior Information Risk Officer (SIRO) and chairs a Technology & Information Board attended by senior IT officers and the Senior Information Governance Officer/Data Protection Officer(SIGO/DPO).

Items regularly reported to the Board include

- Information Security (review national threat level, any local incidents or risks)
- Information governance (breaches, status of work plan, corporate, service data protection documentation and training)
- IT operations update
- IT infrastructure update
- Digital programme update

Information Governance

4.8. The Senior Information Governance Officer/Data Protection Officer (SIGO/DPO) holds the qualification of Associate of the Chartered Institute of Legal Executives (ACILEX) and is currently studying for the BCS Practitioner Certificate (Chartered Institute for IT) in Data Protection. Training and keeping up to date with training is key to delivering a safe system.

4.9. We also have an established network of 35 UK GDPR (data protection) leads across the organisation, who meet regularly with the SIGO/DPO to ensure dissemination of good practice. These "champions" are responsible in their service for ensuring up to date documentation for :-

- Privacy Notices
- Register of Processing Activities
- Information Retention and Disposal Schedules
- Personal Data Breaches (to ensure incidents are being reported)

The SIRO and SIGO acknowledge that the Councils documentation, whilst very largely in place, requires review and improvement and the SIGO is currently undertaking focused reviews with GDPR leads to address this. Annual reviews are recommended by the SIGO/DPO to all GDPR Leads.

4.10. With regard to mandatory information governance training for staff, an online course is available to all computer based staff. All 585 staff have received training (which can be evidenced) in information governance, however there is an issue in ensuring that staff refresh their training regularly. 152 staff have not refreshed their training during 2022 as they should have and these are being actively chased and escalated by our Learning & Development Manager. We are looking to develop a "refresh training" approach, rather than require staff to fully retake the same initial course.

4.11. With regard to the 176 non-computer based staff, in person training is organised for October 2022 (waste and cleansing) and Parks & Foreshore (January 2023) which will provide appropriate and tailored training for the service and will be delivered by the SIGO/DPO.

4.12. It is acknowledged that the audit findings in the planning development service raised concerns about systems of control in a more general sense and a more general audit on information governance has recently been undertaken which is due to report soon. The current SIGO/DPO has undertaken excellent work since coming into post and has really made an impact, improving our culture and practice. We look forward to seeing "where we are" through the general audit, and pushing further forward.

4.13. The SIGO/DPO is following up on completion of recommendations from the planning and development audit

4.14. The work on retention and disposal schedules in planning and development has been completed, Data Protection Impact Assessment training for the service will be completed on September 13th 2022. Reviews of IT contracts in planning will be prioritised by the Digital Contract Managers group described below.

Strategic policy environment

4.15. The Councils have a comprehensive Information Security Policy (April 2022), which is provided as an appendix to this report. This provides policy across a whole range of issues, including Remote Working. The policy addresses issues such as access control, password protection, security of equipment, PCI compliance, security of storage, clear desk policy, information sharing protocols, retention and disposal, internet usage, third party access, data back-up and specific remote access policy.

4.16. The Councils have a comprehensive Data Protection Policy which was last reviewed in February 2022, which is also provided as an appendix to this report. This covers data protection principles, data subject's rights, transfers and disclosures of personal data, privacy notices, registers of processing activity, data security and breach management, data protection impact assessments, officer responsibilities regarding DP governance, contracts, complaints, training and monitoring and approval processes.

4.17. The Councils also have a Blended Working Policy to support the post-pandemic way of working, which sets out a range of employee responsibilities, including UK GDPR and refers staff to the Information

Security and Data Protection policies.

4.18. It is absolutely right for the Committee to highlight the role of "human error" in the risk profile in this area. Personal data breach incidents are reported to the SIGO/DPO for investigation and risk assessments are carried out. Every case is investigated to establish the reasons for the breach and whether the cause is human error or a systematic error. Advice is then provided in terms of containment and mitigation and these details are provided to the Technology & Information Board in detail, and we do seem to be capturing these well with the help of the GDPR Leads/DPO and an improving culture of "no blame, just learn". One such recent incident as an example states, "I inadvertently sent initiative confirmation to the wrong client". We continue to work on ways to improve day to day awareness and embed a culture of good practice and accountability into information handling.

4.19. More detailed information relating to cybersecurity arrangements and training are provided below.

Disaster Recovery

4.20. It is clearly concerning to have received limited assurance in the recent Disaster Recovery audit. In exploring the issue it is important to understand our approach and how risks are being managed through the cloud first strategy alongside significant investment in a major technology refresh in the Town Hall data centre and network.

4.21. There are however some critical improvements being actioned urgently as a result of the audit exercise. A full disaster recovery plan is being brought together to include Town Hall data centre and all cloud services. This is a critical document that is needed as a priority.

4.22. However what follows is an exposition of the arrangements, team knowledge and improvement work already in place and well progressed, which should provide significant reassurance regarding the current position.

4.23. Priority One issues in the audit related to the need for adequate written procedures regarding recovery from an incident at the Town Hall data centre, clear instructions to IT on what systems to prioritise in such a scenario, and a concern relating to there only being a single connection into the Town Hall. These relate to the Town Hall data centre, and in

the next few paragraphs we set the context of the Town Hall facility in relation to our overall architecture and provision.

Cloud first, and the extent of successful delivery since 2015

4.24. The Councils' cloud first strategy was established by the current Director in 2015. This explicitly recognised that there was a need to deliver excellent systems availability, resilience and security by moving systems into the cloud, i.e. away from the Town Hall. By cloud, we mean specialist data centres, run by organisations operating at scale, with extremely high levels of technical skill, resilience and capacity. No Council, especially relatively small ones like Adur & Worthing can be expected to provide such services given the financial and resource constraints they are under. In 2015 this approach was relatively new to the local government sector but is now commonplace and "industry standard".

UK national government policy has advised a "cloud first policy" since 2013, and further advice is set out in the "Cloud Guide for the Public Sector"

"Cloud technology can improve speed of delivery, increase security and create opportunities for organisations to innovate"

and

"Cloud services can have native security advantages over local or on premises technology. ***While organisations can have less visibility of the underlying infrastructure and operations****, cloud providers can use economies of scale to provide a level of security that would be economically or operationally infeasible for many organisations."*

The text highlighted in bold is important to note. When using cloud services it is not the case that the contracting organisation will have visibility of the underlying infrastructure or ability to test it in the traditional way - rather like many other utility or commodity services (e.g. electricity supply infrastructure).

4.25. In the next paragraphs, we set out the extent of cloud-based provision at our Councils, and suggest this provides significant additional context with which to understand the level of risk identified in the audit report. We explore this further below, before returning to the important

improvement actions that are undoubtedly needed.

4.26. It is important for the Committee to know that the large majority of our systems are now cloud hosted in resilient data centres as a result of delivery of the 2015 strategy. This includes:

- Google email, calendar, documents
- Tech One financial management
- Connect HR and Payroll system
- Academy Revenues and Benefits
- Waste management and cleansing
- Tascomi Environment Health
- Orchard Housing Management System
- Home Connections (housing)
- IDOX document management
- Citizen Hub CRM
- Avaya telephone system
- Google Data Studio (data analytics)
- LIFT (vulnerable people) data analytics
- Many others listed in the table at 4.28 below

4.27. Our small team, working with very supportive operational services, has achieved a lot in recent years to make our IT systems much more reliable, resilient and secure.

4.28. The main type of cloud service we use is called “Software as a Service” or SaaS. We contract with a provider, and they promise through their contract with us, to provide disaster recovery for systems and data. Following the audit findings, we are undertaking more work to assemble and manage these contracts and complete a full register of DR arrangements. We plan to establish a “Digital Contract Managers” group in the Autumn.

4.29. Even though the risk is passed to the provider, it is important that we establish this comprehensive register and confirm the precise recovery times for each provider. We hold this information for most key systems centrally, but not all. Checks and deep dives into contracts will be undertaken by the new group.

4.30. Having said this, in practice and in general terms, we know that the recovery times of cloud providers are incredibly quick, often less than two hours and rarely if ever more than 24 hours. The digital team are

involved in procurement and contract activities, as of course are finance, procurement and legal colleagues, ensuring the necessary elements are contained within the contract.

4.31. The contracts that were reviewed by the auditor (Academy Revenues & Benefits and Contact Centre) were deemed to have the required DR arrangements in place.

4.32. Within a SaaS contract, the provider confirms the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The RTO is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. The RPO is the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organisation.

4.33. Below are examples of the DR arrangements that our suppliers are required to provide under contract.

Saas Supplier	Saas product	RTO	RPO	Additional Info.
Capita	Academy - Database failure	12 hrs	12 hrs	Note: In day-to-day running, the SaaS is delivered using multiple redundant systems with in-built high availability designs. For example, all application servers are delivered from a resilient cluster of cloud computing resources that can replace failed resources automatically without user impact. There are two key disaster recovery scenarios, which necessitate a longer RTO: The SaaS is offered from a primary Microsoft Azure Region with all data replicated securely to a second region (for example, UK South and UK West regions). In the event of a major prolonged outage of an entire region, the service would be restored from backup in the secondary region. This is an automated activity, however, can take up to 24hrs from the start of the incident; this is the reason for the RTO of 24hrs.
	Academy - Loss of Azure platform	24 hrs		
	Academy - other system components	4 hrs		
CTS	Google Workspace	0 hrs	0 hrs	Google designs all the components of their platform to be highly redundant, from server design and how data is stored to network and Internet connectivity and even the software services themselves. This “redundancy of everything” includes error handling by design and

				creates a solution that is not dependent on a single server, data centre, or network connection.
Freshworks	Freshservice	4 hrs 12 mins	5 mins	

As indicated in the UK Government Cloud Policy, due diligence with regard to cloud hosting is different to traditional on-premise planning and testing. Each provider publishes documentation and service level agreements that are reviewed as part of due diligence. The RTO and RPO are key and delivered via contractual obligations. The example of Amazon Web Services below indicates how the supplier demonstrates their ability to provide the recovery and backup services required. However, we do acknowledge that a better central grip on digital contracts is required, as mentioned at 4.14. This is being progressed at pace by the Digital Delivery Manager.

4.34. The other type of cloud service we use is called Infrastructure as a Service (IaaS). This approach is typically used where the software provider does not offer a SaaS solution, or where there are technical reasons for local hosting to be preferable, for example the software is not designed to be cloud hosted, and performance (speed) would be too affected.

4.35. Our default IaaS approach is to use a secure and resilient cloud hosting environment provided to the Councils by Amazon Web Services (AWS). We are partnered with a specialist organisation ANS who provide migration services and operational management of the environment.

4.36. We have migrated many of our on-premise workloads to Amazon Web Services (AWS) utilising IaaS architecture. Our on-premise footprint is now much reduced, largely only hosting services that are *required* to be on-prem such as Salto (building management system), or are not suitable for cloud hosting. The AWS cloud services are joined to the on-premise network using a Virgin Media Cloud Connect service, carrying an AWS Direct Connect link (see 4.53 below for further information on links to the Town Hall).

4.37. Because of latency between Worthing and Dublin where our AWS servers are located, some applications (Uniform and Orchard for example) sit behind a Citrix environment, enabling us to access them

through Citrix desktop clients.

4.38. The management of our AWS environment is predominantly undertaken by our contracted specialist supplier ANS, through our co-managed service contract. ANS take care of monitoring and alerting, backups and anti-virus. They will also make requested changes to the environment. ANS also conduct regular best practice reviews.

4.39. As we have a co-managed service in place, AWC still has full access, except for billing, to the AWS environment. We have the ability and some capability to launch and maintain the services we frequently use.

4.40. The table below lists the applications which are hosted in AWS:

Major Applications		**Windows Apps / Databases / SSIS**
IDOX (Planning)	Orchard (Housing)	Capita Balances API
Information at Work (Document Management)	Evidence Link (Video Evidence)	Drawing Register
GIS (Mapping)	Intranet	Enforcement Register
LLPG (Property Gazetteer)	Website	TPO Register (Tree Preservation)
Singlepoint (Addresses)	Avanti (Device Control)	HR Probation Management
Alto (Print Servers)	Land Charges Daily Uniform Transfers Interface	Bacas (Bereavements)
T4 (Site Content Manager)	Forms	LLPG Systems Reports
Recorder (technical Services)	Colony (Allotments)	Safeguarding Management
		Open Data (database and refresher windows app)
		Uniform to Destin data transfer (SSIS)
		Uniform to Northgate M3 Land Charges

4.41. The table shows in more detail just how much of the Councils' operations are now hosted securely in the cloud and not in the Town Hall data centre.

4.42. All of the councils AWS servers are located in Dublin, in what is called an AWS Region, in this case "eu-west-1". This region is made up of 3 independent, geographically dispersed data centres, known as Availability Zones, with AWS services being replicated across all of the Availability Zones in the Region. A general description of AWS infrastructure can be found here:

https://aws.amazon.com/about-aws/global-infrastructure/

4.43. AWC operates servers (instances) in two of the three Availability Zones, giving some level of resilience, should an Availability Zone fail. However, this is extremely unlikely to happen, and if it does, due to ttwonhe serious nature of the issue, and the number of customers affected, AWS will restore services quickly. It is possible to replicate services across Availability Zones and Regions, but this is prohibitively expensive. More information about AWS Service Level Agreements can be found here:

https://aws.amazon.com/compute/sla/

4.44. Should it become necessary for a server instance to be recovered, ANS would manage this process, using a defined procedure to restore a backup in an active Availability Zone.

Town Hall Data Centre and Network Infrastructure

4.45. We fully acknowledge that a written plan is required to guide recovery efforts resulting from a systems outage at the Town Hall. This needs to be undertaken once new infrastructure is in place. We have been at the "tail end" of the old world. Significant investment was approved in 2021 to renew our on-premise architecture and this work is described below.

4.46. Projects delivering the replacement of key infrastructure are well advanced, and when completed will greatly reduce the potential of another outage like that experienced in March 2022 when two

hardware failures caused disruption to some services. This disruption was significantly less than would have been the case if key systems were still hosted at the Town Hall.

4.47. By the end of 2022, a replacement virtual server environment will be in place, and all current on-premise virtual servers will have been migrated to the new hardware. The new system, supplied by Dell, is a modern, hyper-converged infrastructure platform. This makes it easier to support, with available replacement hardware available, should issues occur.

4.48. Along with new server infrastructure, a new backup system will also be implemented. A Dell Data Domain solution will be put in place, consisting of an on-premise appliance, and a virtual appliance hosted in the Amazon Web Services (AWS) public cloud. This new system will eliminate the need for tape backups, and will reduce recovery times. Both Data Domain appliances have the capability to enable server backup images to be “booted up” in a restricted manner, to allow access to applications and data.

4.49. When the new backup infrastructure is installed, as part of the project, the technical elements of a disaster recovery plan for the Town Hall data centre will be developed, including an appropriate DR test regime. Also to be developed are contracts and procedures to cover the unlikely event of the server infrastructure being completely lost. A full corporate disaster recovery plan covering all technologies, on-site and cloud will also provide a register of all cloud hosted software and their DR arrangements. This work is underway and progressing well.

4.50. We do have a clear understanding of the priority services required to be recovered in an incident, and of course these will be built into the new disaster recovery strategy as we establish the “new world” architecture and attendant processes. Priority services are:

- Internet Access
- Google Workspace - Gmail, Calendar, Meet, Drive
- Local Network Shares
- Direct Access
- Academy
- Info @ Work
- Orchard
- TechOne

- IKEN

4.51. It should be noted that another major project is underway and well advanced, being the migration of all files (Word, Excel, pdf documents etc) from traditional on-premise network shares to Google, further improving resilience and improving data management. The digital team next plans to explore data loss prevention tools which will allow additional services for key sensitive files, such as retention and redaction.

4.52. The digital team has also implemented a full backup of our Google data via a service called Druva.

4.53. Closer working with the Councils' Safety & Resilience Manager has been established as recommended by the audit, and regular meetings are now in place.

4.54. Also currently being delivered is a project to replace our Local Area Network (LAN). The current Cisco based infrastructure has served the councils well, but now has some components which are 11 years old. Replacement infrastructure from HP Aruba is being deployed, along with Palo Alto cloud based firewalls, which will move us away from a Town Hall centric model. Other network enhancements will see the provisioning of WIFi 6 and improved guest access.

4.55. The new LAN will complement the connectivity improvements being delivered as part of the "Gigabit" initiative. Our partners CityFibre and MLL are installing Gigabit speed fibres and ISP services. Most important of these being diversely routed connections into the Town Hall Data Centre, eliminating the current single link. This has now been installed and will be commissioned in October.

Cybersecurity

4.56. Cyber risk is one of the Councils' major overall risks. The Technology & Information Board receives routine updates on the national threat level via the National Cyber Security Centre.

4.57. Local government has been an area of risk from the perspective of the NCSC, given the relatively low levels of investment in digital and the dispersed delivery model.

4.58. In January 2022, the Government launched its first ever Cyber Security Strategy, allocating £37.8m to local government. As a result, Adur & Worthing Councils were awarded £100,000 towards improving cyber resilience.

4.59. The cybersecurity audit completed in November 2021 concluded satisfactory assurance. It identified one Priority One recommendation relating to culture, awareness and training. There were also a number of Priority Two recommendations which have been incorporated into an improvement plan.

4.60. During 2022, significant work has been undertaken. The improvement plan contains 29 items, 13 of which have so far been completed. A key recommendation was to recruit a dedicated information security manager and this has been achieved, with a skilled and experienced officer now in post using the £100k funding.

4.61. In terms of cybersecurity training to staff, 80% of all staff have now completed the National Cyber Security Centre learning package, so we are on track for all staff completing the learning in 2022. The Learning & Development Coordinator tracks compliance monthly.

4.62. We have a fully operational IT Risk register that is monitored monthly (Technical Information Board) and additional risks are added when they arise with allocated Owner and updates.

4.63. The audit recommended that the Councils achieve the Cyber Essentials standard. This is an entry level of compliance around cyber security which focuses on the technical overview of cyber security. The Digital team is currently working on the application to have an audit completed to verify compliance and achieve this accreditation. This is an estimated 6 month process.

4.64. Our ambition is to go well beyond this, and over the next year work towards ensuring all our Digital practices are ISO27001 compliant with the potential to seek funds to obtain the ISO27001 certification, one of the highest recognised international Cyber standards. The biggest difference between this and Cyber Essentials is ISO27001 focuses on Policies, Processes and Procedures and not just technical solutions.

4.65. We have purchased a new ITSM tool (Information Security Management System). This platform has all templated Cyber and

Digital Security policies and procedures that are all ISO27001 compliant. This provides a “toolkit out the box” method and will allow us to greatly fast track required improvement around our Cyber Policies and Procedures.

4.66. ISO 27001 is the only auditable international standard that defines the requirements of an ISMS (information security management system). An ISMS is a set of policies, procedures, processes and systems that manage information security risks, such as cyber attacks, hacks, data leaks or theft.

Mobile Device Security

4.67. We have within the last 6 months completed a full technical review and update of our Google MDM service (Mobile Device Management). An MDM is a software solution that adds an essential security layer on all mobile phones and tablets and allows Digital to control what can and can’t be done on the device.

4.68. All Smartphones and Tablets are forced encrypted and forced password protected.

- All smartphones and Tablets can be securely wiped in the event of a lost device.

- We are working on limiting what apps can be downloaded on the Google play store and what websites / applications you can sign in with your google account.

4.69. We are working on a new BYOD Policy and have already implemented security steps to ensure safe usage of corporate Google accounts on personal phones (Work profiles)

4.70. We have implemented regular protocols to seek to prevent phishing attacks. The text below was sent to staff in August 2022 as an example of this work.

“*Digital alongside Learning and Development are working with a 3rd party Cyber security company called BoxPhish, and every month a“test” Phishing email is sent to all staff to monitor the awareness and*

the effectiveness of our cyber training and communications. In August a Phishing test was sent to 527 staff and out of those, 120 staff actually opened the email and clicked the "view document" link in the email. Had this been a real Phishing email then those actions would have put the organisation at risk of attack. Likely attacks would be spreading viruses to disable essential systems or corrupting data and holding it ransom. These types of attacks can take organisations months to recover from. We can and have put multiple security protections on our network to protect our data and systems; however, our greatest vulnerability is staff action.

Several Councils have been attacked in the last few years, and these attacks have been through staff clicking links in phishing emails; it is imperative that we all do what we can to protect our data and our organisation".

Working Remotely

4.71. All corporate laptops are encrypted as standard using Windows 10 Bitlocker

4.72. All laptops connect from home via non corporate network connections using Direct Access (DA), Always on VPN (AoVPN). Both are encrypted end to end and ensure network traffic from the device to our internal network is safe. Before the end of the year, we will be moving to a new solution, delivered as part of the network refresh, called GlobalProtect. This is a cloud based VPN solution, again moving us away from a Town Hall based service.

4.73. All Google accounts have passwords forced with complex password policies and also have 2FA (2 factor authentication) enabled providing robust and secure protection to personal and corporate data stored in Emails and drives.

4.74. A decision was recently taken to enforce two factor authentication into Google at least once a day, and this will be implemented by the end of October 2022. Members and staff alike may find this slightly onerous, and we try to balance our approach to ensure people are enabled - but

this is considered an important protection.

4.75. Staff are expected to adhere to the Council's Information Security Policy and Data Protection Policy when working from home or any other location and the Blended Working Policy confirms this requirement.

5. Engagement and Communication

5.1. In particular, data protection and cyber security issues require ongoing communication and learning. We provide regular updates from the digital team to all staff, conduct monthly tests on staff to maintain awareness regarding phishing attacks, and have developed tailored training to non-computer based staff.

5.2. Our excellent SIGO/DPO is working diligently and robustly to drive adherence to policies throughout the organisation and make sure data protection is at the forefront of minds.

6. Financial Implications

6.1. The Councils regularly invest in technology and digital facilities to ensure that our arrangements are kept up to date to mitigate against risks of data breaches and system failure.

6.2. The move to Cloud based technology significantly mitigates against the risks of both failure and cyber attack but does not remove them entirely. Any such event is disruptive and potentially expensive depending on the nature and duration of the event.

6.3. The Councils have had a computer insurance policy in place for some time to mitigate against risks to the Councils computer equipment and environment. This covers the following risks to our digital environment:

A. Accident.
B. Fire Perils.
C. Residual Breakdown
D. Breakdown.
E. Denial of Access.
F. Failure of Electricity Supply.
H. Failure of Telecommunications.
I. Erasure.

However this is not a full cyber security policy which would insure against the full risks in the event of a cyber attack. Cyber attacks are excluded from our current cover. Such cover would include: cost of investigating a cyber crime; recovering data lost in a security breach and the restoration of computer systems; loss of income incurred by a business shutdown; reputation management; extortion payments demanded by hackers; and notification costs, in the case we are required to notify third parties affected. Such policies, whilst available, are now very expensive.

7. Legal Implications

7.1 Part 2 of The Accounts and Audit Regulations 2015 require the Council to ensure that is has and maintains a sound system of internal controls and governance processes which:-

(a) facilitate the effective exercise of its functions and the achievement of its aims and objectives.
(b) ensures that the financial and operational management of the authority is effective; and
(c) includes effective arrangements for the management of risk.

7.2 Each Council's internal (and external) auditors shall have the like powers set out in the Local Audit and Accountability Act 2014. Each Council shall at all reasonable times (including following the termination for whatever reason of this Agreement) allow or procure for any auditor for the purposes of an internal (or external) audit:

7.3 Section 3(1) of the Local Government Act 1999 (LGA 1999) contains a general duty on a best value authority to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness

Background Papers

- Information Security Policy
- Data Protection Policy
- GDPR Leads - Roles & Responsibilities

Sustainability & Risk Assessment

1. Economic

- The provision of effective digital services to citizens by the Councils supports the economy, for example by enabling the distribution of benefits to residents and the collection of council tax and business rates, among many other services

2. Social

2.1 Social Value

- Issue considered and none identified

2.2 Equality Issues

- Training materials and software systems must be developed with equalities and accessibility in mind.

2.3 Community Safety Issues (Section 17)

- Issue considered and none identified

2.4 Human Rights Issues

- Issue considered and none identified

3. Environmental

- The digital team will increasingly develop policies in line with the Councils' net zero 2030 target in relation to energy use at data centres, ensuring renewable sources and minimising the amount of data stored on servers

4. Governance

- The digital strategy is aligned to the Councils' corporate strategy

- The Technology & Information Board oversee data protection, cyber and other digital and data issues.

ADUR & WORTHING
COUNCILS

ADUR & WORTHING COUNCILS INFORMATION SECURITY POLICY

Document Control

Author	Technology Platforms Manager
Current Version	7.0
Implementation Status	Approved / Implemented
Approved by	Paul Brewer
Date of Publication	04/04/2022
Distribution	All staff via the intranet
Last Reviewed Date	04/04/2022

Revision History

Revision	Date	Author(s)	Description
0.1	30/03/2021	SP	Initial version
0.2	14/04/2021	SD,GA	Revised following review
0.3	20/04/2021	GA	Revised following feedback from MK
0.4	21/04/2021	GA	Revised following feedback from TIB meeting
0.5	31/12/2021	GA	Revised following feedback from BR and M
0.6	25/01/2022	GA	Revised after review of policies and guidance already in place
0.7	04/04/2022	GA	Revised following further comments from MW

1. Introduction

- All information held by the Councils, in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.
- The Policy applies to all Members and employees of the Councils, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by the Councils but engaged to work with or who have access to Councils information, (e.g., computer maintenance contractors) and in respect of any externally hosted computer systems.
- The Policy applies to all locations from which the Councils systems are accessed (including home use, the Councils Remote Working Policy is included in Annex A). Where there are links to enable non-Council organisations to have access to the Councils information, officers must confirm the security policies they operate meet the Councils security requirements. A copy of any relevant third party security policy should be obtained and retained with the contract or agreement.
- Suitable third-party processing agreements must be in place before any third party is allowed access to personal information for which the Councils are responsible.

2. Policy Compliance

- Heads of Service should ensure all staff are aware of and understand the content of this policy.
- If any user is found to have breached this policy, they could be subject to Adur and Worthing Councils Disciplinary Policy, which is available on the intranet. Serious breaches of this policy could be regarded as gross misconduct.
- This policy should be read in conjunction with the Councils' Data Protection Policy

3. Legal Aspects

- Some aspects of information security are governed by legislation, the most notable UK Acts and European legislation are listed below:
- The Data Protection Act (2018)
- UK General Data Protection Regulation (UK GDPR)
- Copyright, Designs and Patents Act (1988)
- Human Rights Act (1998)
- Freedom of Information Act (2000)
- Computer Misuse Act (1990)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications Regulations 2003
- Counter Terrorism and Security Act 2015
- Common law duty of confidentiality

4. Responsibilities

4.1. Manager responsibilities:

- Be aware of information or any equipment which is removed from the Councils offices for the purpose of site visits or home working.
- Ensure staff are aware of and are signed up to the Adur and Worthing Councils Information Security Policy.
- Enforce the Adur and Worthing Councils Information Security Policy when necessary.
- Ensure staff have the appropriate training and knowledge in the use of the equipment.
- Determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.
- Ensure staff are unable to gain unauthorised access to the Councils IT systems or data.
- Determine the security level of any data held or accessed by staff. Review the security level of the data annually and ensure compliance with the current regulations.
- Implement procedures to minimise the Councils exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas.
- Ensure current documentation is maintained for all critical job functions to maintain business continuity in the event of relevant staff being unavailable.
- Ensure staff access to relevant systems is kept up to date. This should be based on changes in roles or responsibilities, as well as staff leaving or joining.
- Ensure that any third-party organisations or contractors providing services for the Councils have understood and agreed to the following:
    - Adur and Worthing Councils Information Security Policy
    - Non-Disclosure Agreement
- Ensure information held is accurate, up to date, and retained, in line with the Councils retention and disposal policy.
- Ensure relevant staff are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, Data Sharing Agreements to which the Councils are signatories and the PSN Acceptable Usage Policy.

4.2. Staff responsibilities:

- Be aware of and comply with the content of the Information Security Policy.
- Ensure any mandatory IT Security and GDPR training is completed as required.
- Ensure that no breaches of information security result from their actions.
- Report any breach of data or suspected breach of data to their reporting manager.
- Report any breach of personal data or suspected breach of personal data to their reporting manager and the Senior Information Governance Officer, without delay.
- Ensure information that they have access to remains secure. The level of security of data and information will be determined by a manager.
- Ensure they are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, or other Data Sharing Agreements to which the Councils are a signatories.

5. Information Security – Data Protection By Design

- The UK General Data Protection Regulation (UK GDPR) requires that organisations put in place appropriate technical and organisational principles and safeguard individual rights. This is known as 'data protection by design and by default'. This means that we have to integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle. The Councils will, therefore, ensure that privacy and data protection, through its Data Protection Policy, is a key consideration in everything they do. As part of this the Councils will:
    - Consider data protection issues as part of the design and implementation of systems, services, products and business practices, using the Data Protection Impact Assessment (DPIA) process to help identify and minimise the data protection risks of a project, before the project commences and at regular intervals throughout the project .
    - Make data protection an essential component of the core functionality of our processing systems and services and utilise the existing resources available on the intranet for Data Protection Impact Assessments.
    - Anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.
    - Only process the personal data that we need for our purpose(s) and that we only use the data for those purposes.
    - Provide training to GDPR Leads to ensure that their Roles and Responsibilities for their respective services are fulfilled.
    - Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:
    - Potential problems are identified at an early stage.
    - Increased awareness of privacy and data protection.
    - Legal obligations are met and data breaches are minimised.
    - Actions are less likely to be privacy intrusive and have a negative impact on individuals.

6. Personal Data Breaches and Information Security Incidents

- The Councils have a duty to ensure that all personal information is processed in compliance with the principles set out in the UK General Data Protection Regulation (UK GDPR). It is ultimately the responsibility of each Director to ensure that their service areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.
- In the event of staff becoming aware of data breach or an information security incident, they are to follow the Councils Personal Data Breach Notification Procedure. Staff must report any breaches or security incidents (suspected or otherwise), by using the Data Breach Reporting Form which will be actioned and risk assessed by the Council's Data Protection Officer.

7. Access Control

- Staff, Members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.
- Access to applications and systems are established based on identity and appropriate group membership. Any access for users or groups will need to be requested through Ask Digital.
- All application access requests will need to be approved, at a minimum, by the reporting manager or team that administers the application or system.
- Any changes to the access level needed by a team or a team member will need to be authorised by the reporting manager or team that administers the application or system and the Information Security team.
- Any access to 3rd party applications or systems by the Councils staff should be established by federated identity to the Adur & Worthing Identity Platform.
- Any 3rd party access to applications or systems will need to be established by the following methods in the order of preference:
    - Federated identity to the 3rd Parties identity platform
    - Creating a distinct group with the 3rd party members that need access to the application or system. There will be a time limit on this, which will be determined by the administrators.
    - Authenticating against the Adur & Worthing Councils RADIUS platform.
    - Locally stored user credentials. In such cases, the locally stored credentials will be temporary and only be valid for a maximum of 24 hours. A service request will need to be raised and authorised by the administrators for every new request.
- The Identity platform will need to comply with Adur & Worthing password guidance which can be found in Annex B.
- Any identification devices, access cards, keys, passes or any item that establishes identity or credentials used to gain access to systems should be assigned on a need basis. The system or application administrators/owners should maintain the list of users that have access to these items, and their direct reporting manager. Any change to the status of the user should be communicated to the application administrator/owner within 5 working days so that the use of the security items can be re-evaluated.
- In the event that an employee leaves the Councils, all access should be revoked by their last working day. The employee's user id in the identity platform should be disabled immediately and deleted within 4 weeks of parting.

8. Security of Equipment

- Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.
- Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.
- Laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.
- Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Council property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.
- Staff working from home must ensure appropriate security is in place to protect Councils equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Councils equipment and information is kept out of sight. The Councils Remote Working Guidance is included in Annex A.
- Councils issued equipment must not be used by non-Councils staff.
- All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the Councils.
- Users will ensure that all sensitive data is either encrypted or password protected.
- Staff and Members who use portable computers belonging to the Councils must use them solely for business purposes otherwise there may be a personal tax or national insurance liability.

9. PCI-DSS Compliance

- The Councils are currently PCI-DSS (Payment Card Industry Data Security Standard) compliant. This is a set of requirements that ensures that all organisations that handle, process, store or transmit credit or debit card information, meet a minimum security standard.
- All changes, improvements, upgrades or projects should ensure that PCI-DSS security standards are taken into consideration and must ensure that the minimum requirements are met.
- The PCI-DSS compliance must undergo annual audit by an external auditor.
- Any member of staff, who has access to any part of the Councils Cash Receipting systems, whereby they are taking payments either in person or over the phone, should only enter card numbers into the relevant payment screens **only**. Under no circumstances should cardholder data such as card numbers be written down, entered or stored in any device or software that has not been approved by the Councils for this purpose.

10. Security and Storage of Information

- All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:
- Paper files stored in lockable cupboards or drawers.
- Laptops and removable storage such as USB hard drives, stored in lockable cupboards or drawers.
- Electronic files password protected or encrypted.
- Restricted access to IT systems.
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must never be left in unattended vehicles
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive or a removable hard drive such as a flash drive or a usb stick. Access to this type of information must always be through the Councils network.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information.

11. Clear Desk Guidance

- Employees are expected to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into locked desk drawers and cupboards as appropriate.
- Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

12. Information Sharing and Distribution

- Any sharing or distribution of sensitive or confidential information must be done using the most secure method available. In Electronic format that would mean using one of the following methods:
    - Cloud Storage: Users may only use official cloud storage solutions to share information with other colleagues or 3rd party vendors. Access to the information must be restricted to user or group identity.
    - Email: Email directed to particular recipient(s) or groups over Transport Layer Security. Any documents attached to the email should be password protected and the password should be sent separately to the recipient(s).

    - SFTP: Secure FTP for larger file transfers. Any use of secure FTP services should ensure there is adequate security set up on the account. The credentials should not be the default credential and the password should comply with the Adur & Worthing Councils Password Policy . The users must ensure that the SFTP service is hosted or approved by Adur & Worthing Councils.
      Unknown or unverified SFTP services hosted on the internet should not be used, as there is no way to ensure that only the intended parties would have access to the data.
    - Physical storage devices: Users may use physical storage devices such as usb disks, or hard drives to share information. This should be considered as the last option, and only used if none of the other options are feasible. Users should ensure that the device is encrypted. The decryption key should be sent to the recipient separately over an encrypted email.
- In the event that information must be shared by post, the information must be sent using a service that can be tracked and that verifies receipt of the items.
- Any information that needs to be printed, should only be printed on Councils owned printers and using the official print solution. Personal or 3rd party equipment should not be used in any circumstances.
- Any information that is printed should be collected immediately and not left unattended.
- Any printer malfunctions that result in the items not being printed, should be cleared off the print queue by the user.
- When disclosing personal or sensitive information to customers, particularly over the phone or in person, the customer's identity must be verified. Service areas dealing with customers on a daily basis should have suitable security questions which must always be used. If in doubt ask for a suitable ID or offer to post the information (to the contact details you have on file).
- In all circumstances, the user must ensure that they are legally allowed to share the information being requested and only share the minimum amount of information necessary.

13. Retention and Disposal of Information

- Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period.
- Please contact the Senior Information Governance Officer for further advice on retention and see the Retention and Disposal Schedules on the Council's intranet.
- When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the shredder waste bins. Electronic information must be permanently destroyed.
- When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage.

14. IT Security

- All IT infrastructure including switches, routers, firewalls, patch panels, servers, storage or any other IT equipment that cannot be considered as end user devices or mobile equipment such as Wireless Access Points, must be secured in cabinets which can be locked.
- All equipment must be rack mounted to the racks. If equipment cannot be rack mounted they should be housed in rackable shelves which can be locked.
- All cabinets should only be accessed by authorised personnel who administer the equipment in the cabinets as well as on site security.
- Possession of the cabinet keys should be tracked either electronically or by a secure register.
- Cabinets should be locked when not being accessed by authorised individuals.
- All equipment should not use default passwords. Any built in credentials should be amended to comply with the Councils password policy.
- IT security should maintain a risk register, with all the security exceptions in place. The items, their justifications and mitigations should be periodically reviewed, and signed off by the ICT & Digital Services Manager.
- Any interfaces on servers, switches, routers, firewalls or any equipment which is not in use should be administratively disabled.
- All IT infrastructure should be built based on standard configuration.
- All groups of IT infrastructure should have standard versions and security controls.
- Any deviation from standards should be noted in the Risk Register, with justification and mitigation of vulnerabilities.
- Networks should be segregated to ensure separation of critical production environments from the enterprise and from the management network used for system administration. Separation between environments can be established as having some form of control that regulates access between environments. This control can be in the form of user authentication, device authentication or network access. Furthermore, within the production environment, access between systems or applications should be regulated.
    - The Enterprise environment is the default environment where every Councils user connects on to. This environment allows access to services such as the productivity suite, general file shares, applications that are open to all users as well as the internet.
    - The Production environment is where services are hosted. These can be services that are consumed by all the Councils employees, specific groups of employees or publicly hosted services accessed over the internet or any other method. Within the production environment, there should be separation to ensure that there is adequate separation between systems. The separation would ensure that only authorised traffic between systems is allowed and any unexpected or unintended communication between systems is blocked.
    - The management environment is where system administrators can manage and administer all the IT infrastructure. This environment would host the network management systems and jumpstations. Administrators would by default be in the Enterprise environment, and would establish a secure connection to the management environment, from where they can administer all of the IT infrastructure.
    - Access to management systems and subsequent access to IT infrastructure will be assigned to users based on identity. Identity will provide the basis for access as well

as the level of access. The use of shared credentials will be limited to read only access. Write privileges can only be assigned to individuals based on their roles.
    - Where possible, local accounts should be disabled or have reduced privileges. Exceptions can be made for root credentials, as due their nature, they cannot be removed or made to have reduced privileges. In such cases, the passwords need to be made sufficiently complex (as per password policy), and made available only to managers.
- Any changes to the configuration of infrastructure should be authorised and tracked. The authorisation and tracking of the changes will be through the Councils change management platform.
- Where possible, encrypted protocols are to be used for management and administration
- All infrastructure will have a method to backup and restore configuration.
- IT support teams will maintain a version history of the backups. The minimum level of version history is 30. This would mean that support staff should be able to roll back to up to the 30th previous version of the configuration or setup.
- All configuration backups, where possible, should be encrypted.
- All configuration backups should only be accessible by authorised personnel. Access should be based on user or group identity.
- All infrastructure should have detailed or debug level logging enabled. Logs should be stored in a remote repository such as syslog or a Security Information and Event Management (SIEM) system.
- All management teams should maintain at least 3 months worth of logs.

15. Internet Usage

- The guidelines for internet usage is applicable to each employee of Adur and Worthing Councils, who require computer and Internet access for their work. Utilising the Internet is allowed and supported as long as the purpose of such usage is to meet the goals of the Councils. Each employee must comply with the rules listed in the policies. Breaching the policies could lead to legal measures taken against the employee. One of these measures is the dismissal from employment. Each of the staff members must realise their responsibility in case of damaging the Councils as a result of such violations. Each employee has to read the policy and comply with it. Any clarifications should be raised with a manager.
- Accepted and supported computer and Internet usage:
    - Internet usage is supported as long as it helps in increasing productivity and it is conducted responsibly. This includes the use of Cloud based productivity tools.
    - All the data shared, posted and received via the Councils equipment belongs to the Councils. It should be managed appropriately and according to the legal policies of the Councils.
    - The equipment available for employees at the working place belongs to the Councils, and its management has all the rights to monitor the Internet activity of all workers. The data transmitted, created and received via the Councils' equipment can be monitored as well.

    - Any website and downloaded content can be monitored by the Councils. They can be banned and blocked by the Councils if considered harmful to productivity and business as a whole.
- Unacceptable ways of using the Internet at the working place:
    - Any communication, including email, SMS and social media post via the Councils' Internet service or on Council equipment that includes any offensive and/or harmful content. Such content includes language and/or imagery that could be considered as harassment or vulgarity.
    - Accessing or distributing harassing, violent, discriminating, hateful or pornographic messages and imagery by the means of Councils equipment.
    - Utilising the Internet and IT equipment at the working place in order to commit any kind of illegal activity, including piracy of music, movies, and other content.
    - Appropriating someone's login information and using it without permission.
    - Illegally downloading, managing or uploading copyrighted content via the Councils IT equipment.
    - Distributing secret Councils information outside the Councils.
    - Posting derogatory information regarding the Councils, its leaders or other employees.
    - Installing inappropriate software that could be harmful to the equipment and network at the working place.
    - Distributing spam emails and posts via the Councils equipment and the Internet.
    - Posting information based on your personal beliefs and presenting it as those shared by the whole Councils.
    - Each employee should consult with their manager or supervisor in the event of not knowing or being unsure about which actions and information are considered unacceptable.
- All the requirements listed above apply to every user of the Councils equipment and network. Any violation of the set rules can result in legal actions taken by the Adur and Worthing Councils against the person violating the policy. Action may be taken under the Councils' Disciplinary Policy.

16. Third Party Access

- No external agency will be given access to any of the Councils networks unless that body has been formally authorised to have access.
- Guidance can be found on the intranet: Data Sharing Agreements and Data Processing Agreements. No external agency will be given access to any of the Councils networks unless that body has been formally authorised to have access.
- External agencies may be required to sign security and confidentiality agreements with the Councils.
- All external agencies processing personal information on the Councils behalf (including via a hosted IT system) will be required to sign a third party processing agreement.
- The Councils will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.
- The Councils will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the

quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

- All third parties and any outsourced operations will be liable to the same level of confidentiality as Councils Staff.

17. Data Back-up

- Data should be held on cloud storage or a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the IT Operations Manager.
- Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.
- All systems administrators should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a usable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is recommended.
- Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The Councils' Retention Schedule must be followed in determining whether data should be archived.
- Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.
- To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.
- Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.
- If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

18. Software

- All users should ensure that only authorised software is in use on their end user devices.
- Where the Councils recognise the need for specific specialised PC products, such products should be authorised by Digital.
- Software packages must comply with and not compromise the Councils security standards.
- Software packages must integrate with the Councils identity platform.
- The Councils seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to Digital.

- Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact Digital for anti-virus advice.

19. Documentation

- All systems should be adequately documented and be kept up to date so that it matches the state of the system at all times.
- System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.
- Distribution of system documentation should be formally authorised by the system administrator. System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.
- Manual data covered by the Gov Connect (GCSX) must not be removed from the Councils offices in accordance with the agreement.

20. ANNEX A - Remote Working

PURPOSE

The purpose of the Remote Working Guidelines is to describe the security requirements for staff remote access connections to internal IT resources.

MS Direct Access provides secure remote access and enhanced management for Windows laptops managed by Digital.

Users are defined as members of staff, consultants or contractors accessing corporate or business systems and using AWC provided equipment.

POLICY

User Responsibilities

1 Access Rights And Privileges

1.1 Remote users are only permitted to access applications and systems they are approved to access for the purposes of fulfilling obligations to AWC.

Remote users must not permit unauthorised persons, including members of their family, to access AWC's computing or information resources from any computers under their control.

2 Information Management

2.1 Remote users must ensure that the collection, creation, use, dissemination and storage of information relating in any way to AWC's business activities is carried out in accordance with internal Policies, relevant best practice Standards or Guidelines and legislation.

As information is likely to be used offsite, special consideration must be given to maintaining appropriate levels of confidentiality and security in accordance with the classification of the information.

3 Connection Requirements

3.1 After a user has completed a remote session with AWC, they must log out.

Hardware and software installed on remote user's computers must not compromise or interfere with AWC's systems. Remote access may be terminated in the event that normal operations are compromised by a remote user.

4 Audit Trails And System Logs

4.1 AWC reserves the right to monitor and audit the use of remote access Connections. Logs containing details of user activities may be retained.

5 Equipment Use

5.1 Equipment supplied by AWC to users is to be operated and maintained in accordance with corporate Policies. The type of use the equipment is put to must not jeopardise manufacturers' warranties and the equipment should be protected against environmental threats and kept secure just as it would be at AWC's premises.

During a remote session the staff member must remain in control of the PC and in front of it so they can see what is going on.

5.4 Remote management of servers, firewalls and other networked devices is permitted providing strong access controls and additional security mechanisms are used. Management of critical devices may not be facilitated via the internet, but must be achieved through back end connections from the corporate network. Where systems are considered sensitive, a user ID and password may not be sufficiently secure and multi-factor authentication, biometrics or other forms of strong access control may be deemed applicable.

6. Digital Services Responsibilities

Access Requirements

6.1 Authentication mechanisms for remote access must appropriately protect the

information or system being accessed. Remote access to systems requires a multi-tiered approach such as logging into the device and a remote access gateway which provides limited network access or multi-factor authentication.

6.2 Users are restricted to applications
and systems that are essential for them to fulfil work obligations to AWC.

6.3 Should an error occur during the authentication process or the user exceed the

number of login attempts, the default setting must be to deny access and the account locked.

7 Encryption

7.1 Remote access links are encrypted by default.

8 Connection Requirements

8.1 When access rights are no longer required, the procedure for termination must be followed. All equipment, hardware, software, etc must be returned and the connection disestablished.

8.2 Systems installed and configured for remote access must not permit any type of real-time in-bound remote access (e.g. telnet, ftp, nfs) unless authorised by the IT Operations Manager. Connections should be achieved through an approved VPN connection or remote access gateway.

8.3 Remote access connections will be installed and configured by authorised IT staff or their agents.

8.4 Where site to site VPN tunnels exist, the tunnel connection will be terminated on the VPN Gateway external logical port and restricted to specific hosts and ports required to support the application. The firewall settings must be forced from the server-side. Users must be restricted to particular systems on the basis of "need to know".

8.5 Network level remote access connections must be terminated through a firewall at both ends of the connection and the appropriate levels of security applied unless the connection is a virtual desktop that prevents processing and storage of information on privately owned or third party equipment. Business to business connections with third parties requires an approved business level firewall.

9 Auditing And Monitoring

9.1 AWC reserves the right to maintain audit logs and monitor remote access connections without notice as and when required to verify systems are working as expected and to ensure compliance with IT Policies.

10 System Support And Maintenance

10.1. System support and maintenance for remote access connections must only be carried out by authorised AWC staff or their designated agents who are technically proficient and understand the implications of specific actions.

11 Training

11.1 Users accessing internal computer systems and information resources by remote access must be educated in the security requirements including how to initiate a access session and gain access to improved systems and how to terminate the when the work is complete.

Correct use of the systems limits the potential for errors and security risks.

21. ANNEX B - Password Guidelines

Passwords are an important aspect of IT security; a poorly chosen password can compromise the security of the Council' critical data and expose the Councils to threats such as unauthorised access, malware and data loss.The below guidelines enforce minimum requirements for both AD and Google accounts to ensure the security of users accounts.

AD Accounts

Password Policy	**Setting**
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	15 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account lockout policy	**Setting**
Account lockout duration	20 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	20 minutes

Google Workspace Accounts

Password Policy	**Setting**
Minimum password length	At least 15
Minimum lower case characters	At least 1
Minimum upper case characters	At least 1
Minimum special case characters	At least 1
Minimum numbers	At least 1
Minimum spaces	No restriction
Google password rating	Strong
Password expiry (sso only)	Every 3 months
Require re-logon to change password	Yes
Warn before password expiry (sso only)	7 days
Password recovery	**Setting**
Enable password recovery	Yes
Force password change in cloud manager	Yes
Allow old passwords	No
No. of old passwords	13
2 step verification	**Settings**
Enabled for OU	Yes
Re-challenge user	On each log in
Mandatory enforced from	Thursday 27th October 2016
New user grace period	1 day

22. ANNEX C - Legislation Relevant To Information Security

Human Rights Act (HRA) – Article 8
Everyone has a right to respect for his private and family life, his home and his correspondence.There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others (legitimate aims).

The Article 8 right is a qualified right and permits public authority intervention when this is:
• in accordance with law,
• in the pursuit of a legitimate aim,
• necessary in a democratic society

Common law duty of confidentiality
Information provided in confidence by a third party is protected under the common law duty of confidentiality, subject to the public interest test.
For personal information to have the necessary quality of confidence it:
• Is not in the public domain or readily available from another source
• Has a degree of sensitivity
• Is communicated for a limited purpose and in circumstances where the individual is likely to assume an obligation of confidence, e.g. health practitioner/patient, banker/customer, solicitor/client, social worker/service user, etc.

Data Protection Act 2018 (DPA) & General Data Protection Regulations 2016 (UK GDPR)

The 2018 Act governs and regulates how personal information is used, replacing the 1998 Act of the same name. It incorporates the General Data Protection Regulations 2016. The Act defines six basic rules or principles, which the Council must adhere to. A breach of any of the principles is a breach of the law.

The Act requires the Council to take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and against the accidental loss or destruction of, or damage to, personal information.

Personal information/data is information about a living individual, who can beI identified from that information.

Special category personal data is defined in the Act as:
• racial or ethnic origin
• political opinion
• religious belief
• trade union membership

• physical/mental health
• sexual life
• commission of offences
• proceedings for offences and sentences of Court
• genetic and biometric data
• location data including IP address

There are additional requirements placed upon the data controller for the processing of special category personal data. A data subject is the individual who the personal information is about. A data controller is the organisation/company legally accountable for the personal data that it obtains, uses, holds, etc. Adur District Council and Worthing Borough Council are the Data Controller for the personal data it processes. A data processor is an individual or organisation that processes personal information on behalf of a data controller and under the instruction of the data controller.

Privacy & Electronic Communications Regulations 2003 (PECR)
The Regulations sit alongside the Data Protection Act. They give people more privacy in relation to electronic communications. There are specific rules on:
• marketing calls, emails, texts and faxes
• cookies (and similar technologies)
• keeping communications services secure
• customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings

Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIRs)

The Freedom of Information Act and Environmental Information Regulations give people the right to ask for access to recorded information held by the Council. Some business information held by the Council will be subject to exemption from disclosure under these Acts. The release of such information into the public domain by whatever means will represent a breach of information security.

Protection of Freedoms Act 2012 (POFA)

The Act enhances individuals' privacy rights in some areas. These include CCTV surveillance and processing biometric data.

Computer Misuse Act 1990

The Computer Misuse Act defines a number of criminal offences, relating to hacking, copying of software, introduction of viruses, unauthorised access or modification of computer material and other similar activities. The Act was amended by Part 5 of the Police and Justice Act 2006 to strengthen the legislation around unauthorised access and penalties for helping others to commit computer misuse.

Counter-Terrorism and Security Act 2015

The Act contains a duty on specified public sector bodies, including councils, to have due regard to the need to prevent people from being drawn into terrorism. This is known as the Prevent Duty. The requirements of the Act are embodied in the Prevent Duty guidance. Extremism is defined in the legislation as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs; or calls for the death of members of UK armed forces, whether in this country or overseas. Radicalisation is defined in the Act as material in support of the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA 2000, and The Telecommunications (Lawful Business Practice) Regulations 2000, provides a framework for monitoring activity, data and persons to assist in the detection and prevention of crime in relation to the Council's work. Interception of data or communications must be relevant, necessary and proportionate.

Copyright, Designs and Patent Act 1988

This legislation gives the creators of materials and information rights to control the ways in which their materials may be used. The legislation places restrictions on the copying and use of copyright material including computer software, publications and images and as such unauthorised copies of information, documentation or software may not be made.

ADUR & WORTHING
COUNCILS

Data Protection Policy

Document Control

Author	Senior Information Governance Officer
Current Version	4.0
Implementation Status	Approved / Implemented
Approved by	
Date of Publication	13/05/2020
Distribution	All staff and public website
Last Reviewed Date	23/02/2022

ADUR & WORTHING
COUNCILS

1. Purpose

The purpose of this policy is to ensure appropriate measures are applied by the Adur & Worthing Councils to comply with the data protection legislation, namely, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), as well as the Information Commissioner's Office (ICO) guidance.

2. Scope

The Councils are committed to compliance with all data protection legislation in respect of personal data and the protection of the rights and freedoms of individuals whose information the Councils collect and process.

This policy applies to all staff, elected members, contractors and any other persons who have access to the Councils' information, information systems and networks.

This policy applies to all personal data processed, i.e. held, created, modified, accessed or shared, from the effective date of this policy. It includes personal data in any form, no matter whether it is stationary (e.g. an electronic or paper document) or in transit (e.g. file transfer, email, fax, phone, post). It also covers the Councils' buildings, premises and systems which contain that data.

3. Policy Statement

The policy sets out the Councils' commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data. The Councils are committed to:

- Ensuring that we comply with the data protection principles;
- Meeting our legal obligations as laid down by the data protection law;
- Ensuring that personal data is collected and used fairly and lawfully;
- Processing personal data only where necessary in order to meet our operational needs or fulfill legal requirements;
- Taking steps to ensure that personal data is up to date and accurate;
- Establishing appropriate retention periods for personal data;
- Ensuring that data subjects' rights can be appropriately exercised;

- Providing adequate security measures to protect personal data;
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues;
- Ensuring that all staff and Members are made aware of good practice in data protection;
- Providing adequate training for all staff and Members responsible for personal data;
- Ensuring that everyone handling personal data knows where to find further guidance;
- Ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly;
- Regularly reviewing data protection procedures and guidelines within the organisation.

4. The Principles of Data Protection

The GDPR states that anyone processing personal data must comply with seven principles. These principles are legally enforceable.

The principles at Article 5(1) UK GDPR require that personal information:

1 Shall be processed lawfully, fairly and transparently

The Councils will:

- Ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful.
- Only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing.
- Ensure that data subjects receive full privacy information so that any processing of personal data is transparent.

2 Shall be processed specifically, explicitly and legitimately

The Councils will:

- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice.

- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

3 Shall be adequate, relevant and not excessive

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- The Councils will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

4 Shall be accurate and kept up to date

- The Councils will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

5 Shall be kept for no longer than is necessary

- The Councils will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

6 Shall be processed in a manner that ensures appropriate security

- The Councils will ensure that there are appropriate organisational and technical measures in place to protect personal data.

7 The principle at Article 5(2) UK GDPR require that the Councils shall be able to demonstrate compliance with the above

The Councils will:

- ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request.

- carry out a Data Protection Impact Assessment (DPIA) for any high risk personal data processing, and consult the Information Commissioner if appropriate.
- ensure that a Data Protection Officer (DPO) is appointed to provide independent advice and monitoring of the Councils' personal data handling, and that this person has access to report to the highest management level of the Councils.
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law. The GDPR provides conditions for the processing of any personal data that must be met. It also makes a distinction between personal data, "special category" (sensitive) personal data and criminal conviction personal data. Special category personal data requires stricter conditions for processing.

5. Data Subjects' Rights

Data Subjects have the following information rights with regards to the Councils processing their personal data, subject to any exemptions or exceptions:

- To be informed about the collection and use of their personal data;
- To access and obtain a copy of their personal data;
- To withdraw any consent(s) given for processing at any time;
- To have personal data erased in certain circumstances;
- To request the restriction or suppression of processing in certain circumstances;
- To obtain and reuse their personal data for their own purposes across different services in certain circumstances;
- To prevent processing for purposes of direct marketing;
- To object to the processing of their personal data in certain circumstances;
- To not have significant decisions that will affect them taken solely by automated process unless in certain circumstances;
- To seek remedy in a court of law if they suffer damage by any contravention of the UK GDPR and/or the DPA;
- To request the supervisory authority (ICO) to assess whether any provision of the UK GDPR and/or the DPA has been contravened.

6. Transfers and Disclosures of Personal Data

In order to provide services and to meet our legal obligations as a local authority, the Councils will sometimes need to share your personal information with external organisations.

We will only share your personal information where it is necessary, either to comply with the law or where permitted under data protection legislation.

Examples of organisations, we may share your personal information with:

- NHS
- HMRC
- Police
- UK government departments, and related agencies
- other local authorities
- Ombudsmen, the ICO, the Care Inspectorate
- Care providers and voluntary organisations

For more information about who we share your personal data with and why, please see 'Service Related Privacy Notices' which can be found on the Councils' website.

The Councils only share your information with partners or contractors who agree, through Data Sharing/Processing Agreements, to protect your information.

Sharing information outside of the UK

Almost all personal data the Councils use is stored and processed in the UK. Some information may also be stored within the EU.

If we need to transfer your personal information outside of these areas for a particular activity, this will be explained in the relevant service-specific privacy notice together with a description of the protective measures we have put in place to keep it safe.

Any transfer of personal information between the Councils and partner organisations shall be carried out using a secure method agreed by the Councils' ICT Services.

7. Privacy Notices

The Councils shall ensure that a corporate privacy notice is published on the Councils' website. It shall explain in general terms:

- what information is being collected;
- why the Councils collect information;
- who the Councils may share this information with;
- what the Councils will do with the information;
- how long the Councils will keep the information;
- what rights individuals have
- how to contact the Councils' Data Protection Officer

  (data.protection@adur-worthing.gov.uk)
- how to contact the ICO

  by post at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or phone 0303 1231 113.
- You can also make a complaint or find out more information on the Commissioner's Office website.

Where relevant, service areas shall provide their own privacy notice(s) confirming this information in specific terms.

8. Register of Processing Activities (ROPA)

The Councils will:

- Record processing activities in electronic form so you can add, remove and amend information easily.
- Regularly reviews the record against processing activities, policies and procedures to ensure that it remains accurate and up to date, and you clearly assign responsibilities for doing this.
- Regularly review the processing activities and types of data you process for data minimisation purposes.

- Ensure that effective processes are in place to keep the record up to date, accurate and make sure that the data is minimised.
- Ensure that staff can explain their responsibilities and how they carry them out in practice
- The ROPA includes (as a minimum**)**
    - organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
    - the purposes of the processing;
    - a description of the categories of individuals and of personal data;
    - the categories of recipients of personal data;
    - details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
    - retention schedules; and
    - a description of the technical and organisational security measures in place.
- An internal record of all processing activities carried out by any processors on behalf of your organisation.

9. Data Security and Breach Management

The Councils shall ensure that it processes personal data securely by means of appropriate technical and organisational measures.

- These measures will include adherence with relevant Council policies
- Access to personal data shall be strictly controlled.
- The Councils shall investigate all suspected breaches which involve personal data.
- Where a breach is identified, this will be reported to the ICO where necessary, based on UK GDPR requirements.

10. Data Protection Impact Assessments

- A data protection impact assessment (DPIA) is a process to help the Councils identify and minimise the data protection risks of a project.

- The Councils will conduct a DPIA for major projects which require the processing of personal data or where processing is likely to result in a high risk to individuals' interests, rights and freedoms.

11. Responsibilities

This section should be read in conjunction with the responsibilities detailed in Councils' other Information Governance and Security Policies. Additional responsibilities arising from this policy are specified below.

11.1 Data Protection Officer

A suitably qualified and experienced Data Protection Officer will be appointed to undertake their statutory duties:

- to inform and advise the Councils and employees about their legal obligations under the UK GDPR and DPA and other data protection laws;
- to monitor compliance with the UK GDPR and DPA and other data protection laws, and with the Councils' data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, Data Protection Impact Assessments;
- to cooperate with the ICO;
- to be the first point of contact for the ICO.

In addition the Data Protection Officer will be responsible for:

- Keeping a central catalogue of service areas' Registers of Processing Activities;
- Manage and report as appropriate any personal data breaches;
- Advise the Councils on Privacy By Design;
- Annual renewal of notification ICO registration.

11.2 Senior Information Risk Owner

Is responsible for oversight of compliance and risk management.

11.3 CEO and Directors

The CEO and Directors are ultimately responsible for overseeing and ensuring compliance with this policy and data protection legislation.

Directors are responsible for ensuring that their respective services are complying with the data protection legislation and that relevant data protection and information governance and security policies and procedures are enforced.

11.4 Heads of Service and Service Managers

It is the responsibility of managers to ensure compliance with this policy within their own service areas. Their responsibility includes:

- Ensuring that staff are aware of their responsibilities under the data protection legislation and follow information governance best practice;
- Ensuring employees, including contractors, consultants and volunteers employed to undertake Council business follow the Data Protection Policy and procedures;
- Ensuring that compliant contracts with Data Processors are in place;
- Ensuring that service areas' Registers of Processing Activities are maintained and updated regularly;
- Ensuring that service areas' Privacy Notices are maintained and updated regularly;
- Ensuring that service areas' Information Retention and Disposal Schedules are maintained and updated regularly;
- Ensure appropriate resources are in place to enable compliance with the Data Protection Policy;
- Ensure that compliance with data protection legislation under the DPA, UK GDPR, any other data protection legislation and good practice can be demonstrated.

11.5 Staff

All staff:

- Must be aware of the data protection legislation and of their obligations under it;
- Individual staff members may be personally liable for privacy breaches if they act outside the authority of the data controller;
- All new members of staff must undertake data protection training and familiarise themselves with the Councils' Data Protection Policy and procedures as part of their induction process and in training sessions provided by the Councils;
- Refresher training will be carried out for all staff on a regular basis, in particular when there are any changes in legislation, when there is a significant information security incident or on a yearly cycle at the Councils' discretion;
- Report personal data breaches to the Data Protection Officer as soon as possible.

11.6 Elected Members

All Elected Members:

- Should be made fully aware of this policy and of their duties and responsibilities under the data protection legislation;
- When handling personal data in their role as politicians (e.g. when out canvassing), Members should be complying with the rules and requirements of their respective political parties and their Data Protection Policies;
- When acting in their role as Elected Members, they should be complying with the Councils' Data Protection Policy. As such, they have to handle personal data in line with the requirements of the Councils' Data Protection Policy.

12. Contracts

- All Council contracts shall include appropriate terms to ensure that personal data is handled in accordance with the Data Protection Act 2018 and the UK GDPR.
- Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be used or disclosed for any other reason.
- The Councils shall ensure that before personal data is shared with a third party as part of a contract that appropriate technical and organisational security controls are

in place.

13. Complaints

All complaints regarding Councils' handling of information rights requests will be dealt with by the Data Protection Officer or an appropriate nominated senior officer. The Councils will make available details of the complaint procedure to applicants. Complaints will not be handled by persons who participated in the original decision.

Complaints and requests for review should be submitted by the applicants to the Data Protection Officer within three months of receipt of the initial response.

Where the Councils' procedure upholds an initial decision, the applicant will be advised of the right to appeal and the steps involved to take the matter to the Information Commissioner.

14. Training associated with this Policy

Compulsory online training is provided to staff via Adur & Worthing E-Learning. Online training will also be provided to Members.

Additional workshops for staff and Members will also be organised by the Senior Information Governance Officer (SIGO) and the Request for Information Officers (IO). Various guidance is available on the Intranet.

If anyone requires support, advice or guidance on any element outlined in this policy they should speak with their line manager in the first instance.

15. Monitoring

Compliance monitoring will be carried out by the Councils' Data Protection Officer and through the Councils' management structure.

Disciplinary action in accordance with procedures approved by the Councils may be taken against any employee who violates the requirements of this policy.

This Data Protection Policy will be reviewed annually by the Data Protection Officer.

16. Related documents

This policy should be read in conjunction with the following documents:

- Other policies in the Digital's Information Security Policy Suite;
- Any supporting standards, guidelines, processes and procedures.

17. Approval process for Data Protection Documentation

- In order to achieve and maintain control of documentation, any reviews and/or changes to data protection documentation (ROPAS/Privacy Notices/Retention and Disposal Schedules) may only be carried out and approved by the GDPR Lead or Head of Service within their own service block.
- (E.g. The GDPR Lead for Planning is responsible for approving and reviewing any changes in respect of Planning Services only).
- Data Protection documentation(ROPAS/Privacy Notices/Retention and Disposal Schedules) shall be reviewed annually by the GDPR Lead or Head of Service and in consultation with the Data Protection Officer to minimise the risk of problems and adverse impact on services.
- Each time a document such as a ROPA/Privacy Notices/Retention and Disposal Schedule is reviewed and changes made, this must be documented by a version control for each document. This must state:
    - The date the document is reviewed
    - the version number
    - the notes/reasons for the changes and
    - the name of the person who has reviewed the document.

18. Document History - Version Control

Version	Date	Notes/Reasons	Reviewers
2.1	April 2018	Unknown - history not recorded - ISPS-011	IS Project Team
3.0	06/02/2020	Policy updated to bring in line with current legislation. Formatting changed. Links & ref to JONG added. Responsibilities for SIRO,	SIGO

		CEO and Senior Managers added. Members' responsibilities updated - requirement to register with the ICO removed. Complaints procedure added. Version Control table added.	
3.0	13/05/2020	Agreed by JONG. Finalised for publishing.	SIGO
3.0	28/04/2021	Policy reviewed. Refs to 'GDPR' replaced with 'UK GDPR'. Ref to 'Information Officers' replaced with 'Request for Information Officers' as per formal title.	SIGO

Appendix A - Glossary

Personal data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health (including mental health) or data concerning a natural person's sex life or sexual orientation.

Data Subject – an identified or identifiable natural person from the personal data held by an organisation.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the Data Controller to report personal data breaches to the ICO and where the breach is likely to result in a risk to people's rights and freedoms.

ADUR & WORTHING
COUNCILS

GDPR Leads - Role and responsibilities

Who are the GDPR Leads?

AWC has established a network of 35 GDPR Leads across both councils.

This is required to ensure the GDPR compliance across the AWC. To put it simply, GDPR Leads are our 'data protection champions'!

A list of GDPR Leads is available on the Intranet.

What are the GDPR Leads expected to do?

- Be the first point of contact for colleagues regarding any GDPR-related queries
- Be able to inform and signpost colleagues
- Know the GDPR governance framework procedures (***currently being updated***)
- Note any gaps in knowledge or breakdown in procedures
- Ensure that procedures are followed in their service area, especially by maintaining and/or updating the service area's:
    - Privacy Notices
    - Register of Processing Activities
    - Information Retention and Disposal Schedule
    - Personal Data Breaches (to ensure incidents are being reported)
- Support the Senior Information Governance Officer (SIGO) and notify of any issues/updates
- When stepping down from the role, to ensure there's a hand over to the new Lead

What support is available from SIGO to the GDPR Leads?

- Information, advice and guidance
- Regular workshops and training sessions, healthchecks
- Reviewed and updated procedures, central repository
- 1-to-1 sessions upon request
- Networking opportunities

Any questions? Come speak to the SIGO or email data.protection@adur-worthing.gov.uk