READING BOROUGH COUNCIL

ICT SECURITY POLICY STATEMENT

April 2019 Version 1.7

Version No.	Date	Change Description	Approved By
1.0	04.04.12	Revised for new Organisational Structure.	ISPB
1.1	01.04.13	Revised for new Organisational Structure, and Information Governance.	ISPB
1.2	17.11.14	Revised for new Organisational Structure, and Information Governance compliance 27001/2013, Partner & Third Party compliance, PSN GCSx Additions, NFI Fraud, PCI DSS.	ISPB
1.3	24.02.15	Revised for new Organisational Structure & Policy Document References.	CMT
1.4	06.08.15	Director Changes	CMT
1.5	01.08.16	Revised for MD & Director Changes, Official-Sensitive data, Information Asset Register, N3 Network compliance, Ransomware, Cyber Crime.	ISSG
1.6	01.04.18	Update references to other documents	CIGB
1.7	23.04.19	Revised for new Council structures, GDPR, & CIGB change, Cyber Threats & training, PCI DSS, IG Roles, Vulnerability Monitoring, Data Retention, Mobile Devices, Third Party Control, Secure Email Blueprint adoption, On-boarding / Off-boarding of staff.	CIGB

All revisions agreed by the Corporate Information Governance Board and formal consultation processes of the Council will be notified to Employees, Councillors and other Organisations as identified within this Policy Statement

THIS POLICY STATEMENT SUPERSEDES ALL PREVIOUS STATEMENTS MADE BEFORE April 2019

INTRODUCTION

Information and Communications Technology (ICT) is now an integral part of every area of the Council's service delivery, and the integrity of all data (whether in electronic or paper formats) is of vital importance to the continued efficient operation of all Council services and therefore must be subject to formal management and controls.

The risks to the Council through data security problems are varied, but these all ultimately relate to the continued ability of the Council to operate effectively and credibly.

Typical risks range from the physical loss of corporate and service systems through disaster scenarios, loss of a specific business function through a database corruption or data loss, financial loss from litigation or fines imposed for data related incidents (the Information Commissioner can impose fines of up to E20m without appeal), to loss of Council credibility due to a 'leak' of confidential information or inappropriate public access to private data. Loss of public confidence in the Council's security and information governance processes would also undermine the realisation of financial savings expected from the Council's Customer Access Channel Strategy and Transformation Programmes where residents are provided with choices to contact the Council through lower cost access channels and receive a consistent quality of service.

In addition there are ranges of potential external and internal criminal activities that must be identified and controlled through a risk based approach. As internet based crime is becoming more sophisticated, internationally directed and tool kits to undertake this activity are readily available on the internet, it is essential that awareness levels to mitigate new threats is actively promoted and security is actively reviewed and evolved to offer continuing protection.

The evolving business requirements of the Council involves the exchange of data and information between the public and private sectors, and with public sector initiatives towards "Big Data" handling (high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making), increasing security controls needed for Credit and Bank card secure handling, with an increasing threat of Cyber-attacks locally, nationally, and internationally. This all brings a greater need to comply with Information Security Standards, Information Governance and recognised ICT best practise to be able to ensure the continuity of Public and Private Sector Services adequately protected from threats and compliant with UK Law.

OBJECTIVES

The purpose of this policy is to formally state Reading Borough Council's commitment to the principles of ICT Security (ISO 27001/2013) and ICT Governance and to promote their integration into operational processes across the entire organisation.

All Employees, Contractors & Casual Staff are expected to comply with the Council's **Information Security and ICT Use of Equipment Policy** and **Information Governance processes** unless a specific exemption has been both allowed and recorded. Council Staff are expected to act professionally at all times and be responsible for their own actions, including the actions of anyone logged in as them. Disciplinary action may result from non-compliance.

All Councillors are expected to comply with the **Information Security and ICT Use of Equipment Policy** and **Information Governance processes** and the Code of Conduct for Councillors as issued by the Council. A Councillor, when using or authorising the use by others of the resource of the Council must:

(i) Act in accordance with the authority's requirements;
(ii) Ensure that such resources are not used for political purposes as agreed in the Code of Conduct.

A Councillor must not, in his/her official capacity, or any other circumstance, conduct him/herself in a manner that could reasonably be regarded as bringing his/her office or the Council into disrepute. Breaches of the Council's Policies as defined for Councillors will be referred (subject to the seriousness of the breach and whether this in turn breaches the Code of Conduct for Councillors) to the Leader of the Council/Group Leaders for investigation (Stage 1), the Head of Legal Services (Stage 2) and the Local Standards Committee (Stage 3) for appropriate disciplinary action.

This Policy Statement is supported by the Information Security Policies and associated guidance issued to employees, councillors and organisations contracted to work on behalf of the Council. In particular, requirements, responsibilities and sanctions are defined within the **Information Security & ICT Use of Equipment Policy,** (with key points summarised for easy digestion into the **ICT Security Golden Rules** handout) which is a joint agreement incorporated into contracts of employment and contracts for services.

The systems used to maintain access to data and data security are a combination of physical and digital applications, operational procedures, formally recorded training, scrutiny and audit checks.

This document is an integral part of the overall Corporate Governance of the Council, which extends structured information management procedures to all data (digital or manual) that is processed by or on behalf of the Council.

READING BOROUGH COUNCIL POLICY STATEMENTS

The Council:

Business & Personal Use

- Has provided ICT systems for **Council business use** and therefore there are no rights of personal use or individual privacy outside those specifically granted and defined within the documentation accompanying this Policy Statement (for staff this is defined in the **Information Security & ICT Use of Equipment Policy).** The Council will monitor systems accordingly to enforce the ICT policies.

Information Management

- Is committed to open and effective information management and to the processes required to ensure that the security of all data is maintained;

- Recognises all information, (whether in electronic or non-electronic formats), are assets fundamental to the continued delivery of services by the Council and therefore must be managed and controlled as such;

- Recognises the need to comply with all relevant UK Legislation (including the Data Protection Act 2018 - incorporating the EU General Data Protection Regulations GDPR revisions) and the increasing potential threats to information assets through security breaches, and will therefore put in place and comply with information security standards across the whole Council together with the adoption of ICT Security Golden Rules;

- Recognises the delivery of secure information management needs to be considered and scoped in to all contractual undertakings with Third Parties where this is relevant;

- Recognises the importance of information security management and governance to the continued operational viability of the Council, its partners and all other organisations affected by its undertakings;

- Will undertake to classify information assets to ensure appropriate controls and protection measures are in place for sensitive information, will ensure Information Asset owners are appointed and trained and an Information Asset Register is maintained to record the Councils Information Assets, and will ensure the retention and disposal of all data is undertaken in accordance with legislative requirements;

- Will ensure the appropriate treatment of all data within the Governments Document Management Classification scheme and adhere to security requirements expected of handling data up to OFFICIAL-SENSITIVE levels as a Local Authority;

- Will ensure the marking of emails and documents in accordance with the Governments Document Management Classification Scheme (OFFICIAL, OFFICIAL-SENSITIVE) and as a risk mitigation action for Data Protection compliance with sensitive data.

Corporate Processes & Governance

- Have set up a Corporate Information Governance Board Chaired by the Senior Information Risk Officer (SIRO) who are charged with the implementation and on-going review of the Council's ICT Security Procedures and ICT Security Incident recording to ensure Security Procedures are refined and Security Incidents are recorded, investigated, and remedial measures put in place as is necessary;

- Will undertake to review Job Descriptions to ensure responsibilities as ISO 27001/2013 and Data Protection Information Asset Owner responsibilities are appropriately assigned within the Council;

- Will undertake to appoint a senior officer to act as a Senior Information Risk Owner (SIRO) for the Council who will report to the Councils Senior Management Team to ensure appropriate focus and consideration of Security and Information Governance in Corporate Decision making;

- Will undertake to appoint a Data Protection Manager who will report to the SIRO and attend the Corporate Information Governance Board to oversee Data Protection compliance across the Council;

- Recognises the need for ICT Governance to integrate with the Council's overall Corporate Governance, integrating the Council's ICT and Business Strategies to deliver best value services of a consistent high standard and quality;

- Recognises the need for continued support for ICT Security and ICT Information Governance awareness raising across the organisation to avoid ICO fines and continued compliance with UK legislation;

- Will provide appropriate professional training for key security roles (SRIO, Data protection Manager, IT Security Manager, Information Asset Owners, Caldicott Guardian);

- Will integrate information security management into all levels of Service Planning and Service delivery;

- Will undertake annual Risk Management assessments and implement appropriate measures to control the identified risks seeking to minimise the risk of damage to operations, loss of reputation and costly litigation;

- Will ensure proper accountability of both hardware, software and information (both electronic and manual) assets;

- Will undertake regular independent Network / Server / Desktop and Smartphone Vulnerability Assessments and undertake associated remedial action to mitigate any risks uncovered;

- Will ensure capacity planning and testing processes form part of overall ICT management;

- Will ensure Disaster Recovery measures are in place for all critical and important systems;

- Will ensure Services put in place and annually review Business Continuity Plans to sustain their operations;

- Will set up information sharing protocols (or equivalent) to control the movement of information within the Council and to external organisations and partners;

- Will ensure Joiner/Leaver processes are in place for on-boarding/off-boarding of all categories of workers;

- Will ensure proper training and induction of all staff including Heads of Service in the appropriate secure use of ICT and Data Protection compliance within the Council, and their Information Governance responsibilities;

- Will actively promote Security Awareness and Information Governance within daily operations to embed continuing best practice within the culture of the Council;

- Will ensure all staff are aware of their Personal Commitment responsibilities when accessing PSN services and where necessary have been appropriately Baseline Personnel Security Standard Checked to access such services;

- Will ensure staff are aware of their personal responsibilities when accessing the NHS N3/HSCN network and will only do so on a role based access approved basis;

- Will ensure appropriate control measures are in place to handle data securely up to impact OFFICIAL-SENSITIVE levels;

- Will ensure the appropriate application of Document Making Standards on all email and documents;

- Will ensure appropriate data retention policies are applied appropriately to council data assets;

- Will ensure appropriate control measures are in place in accordance with PCI DSS regulations to protect bank / credit card data;

- Will ensure Banking Processes are appropriately authorised and overseen by Finance and PCI DSS compliance is maintained on any new arrangements entered into.

<u>Security Benchmark Standard</u>

- Will work towards achieving Council compliance with ISO 27001/2013 for Information Security Management (the recognised security standard of both the public and private sector).

Legislative references

- Will comply with all relevant UK legislation including:
    - The Data Protection Act 2018 *(as revised by GDPR May 2018);
    - The Freedom of Information Act 2000;
    - The Human Rights Act 1998;
    - The Computer Misuse Act 1990;
    - The Electronic Communications Act 2000;
    - The Copyright Designs & Patents Act 1988;
    - The Regulation of Investigatory Powers Act 2000;
    - The Disability Discrimination Act 1995;
    - Caldicott Guidelines (DOH);
    - Race Relations Act;
    - Sex Discrimination Act;
    - The Environmental Information Regulations (2004);
    - NIS Regulations (The Network and Information Systems 2018);
    - Privacy & Electronic Communications Regulations (2018).

    And such other relevant legislation as from time to time may be enacted;

- Will ensure compliance with all relevant software licensing best practice procedures.

Local Policy references

- Will ensure the enforcement, compliance and continuing management of Information Security and Information Governance through the linking to relevant Council Polices and Procedures including:
    - The Code of Conduct;
    - Whistle blowing Policy;
    - Grievance & Disputes Procedure;
    - Customer Care Handbook;
    - Data Protection Policy (including Subject Access Request Procedures);
    - Breach Management Policy;
    - Records Management Policy;

- Procedure for dealing with Requests for Information (FOI)
- Information Sharing Policies
- Document Retention Schedules
- Equality and Diversity Procedures
- Joiner and Leavers Procedures
- NFI Fraud Initiative
- PCI DSS Bank Card Handling
- Information Security and ICT Use of Equipment Policy
- ICT Information Risk Management Document Marking Policy
- ICT Standards Expected of Third Parties Policy
- ICT Camera & Video Usage Policy
- ICT Huddle Acceptable Use Policy
- ICT Removable Electronic Media Usage Policy
- ICT PSN Personal Commitment Policy
- ICT PCI DSS Personal Commitment Policy
- ICT Security Golden Rules
- ICT Controls for Storage & Carriage of Hard Copy Documentation
- Internet Monitoring Policy
- Email Monitoring Policy
- Caldicott Guardian Compliance Monitoring

Council Responsibility

- Will ensure all employees, councillors and contracted third parties (e.g. contract staff, casual staff, consultants, partner organisations) are aware of their individual responsibilities and accountability, and sanctions for breach, within this policy. This will be achieved through the **Information Security & ICT Use of Equipment Policy;**

- Will ensure the roles of SIRO, Data Protection Manager, IT Security Manager, IT Auditor, Caldicott Guardian and Information Asset Owners and Data Processors are allocated and those Information Governance responsibilities discharged appropriately throughout Council Processes;

- An easily digestible **ICT Security Golden Rules** document will be made available to summarise key information for all employees and councillors to aid compliance;

- Will provide to all employees and councillors training, information, and adequate supervision to enable them to comply with their own duties within the security policy of the Council;

- Will provide advice and guidance to external organisations on the Security Expectations the Council has when working with them. This Guidance is contained in the document **ICT Standards Expected of Third Parties.** This includes specific expectations on secure gateways and firewalls are in place such as to protect both the Council and the PSN and N3/HSCN networks.

- Information Asset Owners will undertake risk and Privacy Impact Assessments for any key changes in their operational environments to safeguard Information Assets and Processes on-going;

- Will undertake to review and update (whenever necessary but as a minimum annually), this document, the **Information Security & ICT Use of Equipment Policy, ICT Security Golden Rules** and other associated documentation and will communicate any changes to all necessary parties, subject to consultation and negotiation on any changes to joint agreements / staff policies and guidance;

- Will charge the Councils Senior Information Risk Officer and CICTS with the responsibility for monitoring and reviewing security on-going (including security incidents) and for further developing and reviewing the policy and standards. Recommendations for changes to policies affecting staff will be consulted and negotiated through normal Council routes;

- Will ensure appropriate configuration and use of security software and controls (e.g. use of Firewalls, Virus and Malware software protection, Log monitoring, Secure email, Laptop and server encryption, Security Incident Event Monitoring and Security Operational Procedures for Security etc.) to safeguard the Councils Information and operations;

- Will ensure Major Incident Plans are in place to protect the Council for foreseeable threats (including those emerging from the Cyber landscape).

- Will promote employee awareness for general security controls including clear desk, clear screen, secure remote working, secure email, secure transmission and movement of data, movement of ICT assets and the decommissioning and disposal of information and ICT assets;

- Will alert staff and councillors to new threats when the council is made aware of vulnerabilities that could affect both business and personal operations;

- Will ensure all council staff accessing the N3/HSCN network will do so on a role based need and will adhere to the operational standards and accreditation as required by the NHS;

Integrity of Information

- Will consider all data to be key assets of the Council and will manage them as such;

- Will ensure the main principles of the Data Protection Act 2018 (as revised under GDPR) are adhered to including that all data (whether electronic or non-electronic is maintained so as to ensure it is always up to date, relevant, accurate and secure;

- Will ensure its core case management systems are updated in a timely manner to reflect changes the Council receives;

- Will ensure the accuracy, quality, and appropriate retention of the data held in its Case Management Systems;

- Will appropriately manage any sharing of Council Information Assets with Third Parties so as to ensure the appropriate protection of that data at all times, including putting in place appropriate Information Sharing Protocols, Privacy Impact Assessments and the publishing of Fair Processing Notices to the Public to ensure transparency of data usage.

Access to Information

- Will ensure electronic data, and data held on mobile devices, (including the transmission of data across the internet) is protected by appropriate security mechanisms;

- Will put in place appropriate security mechanisms to regulate and manage the connectivity of peripheral devices e.g. hardened passwords;

- Will classify information assets to ensure only appropriate access is given on a role based need;

- Will ensure ICT systems hardware is appropriately located and managed so as to maintain secure service availability;

- Will ensure secure access to ICT systems is maintained by appropriate use and control of user names and "hardened" passwords;

- Will ensure key information such as access codes or contact details are never entrusted to a single individual without further contingency measures being put in place to maintain business continuity;

- Will ensure automatic timeout and disconnection procedures are implemented to protect against unauthorised access;

- Will ensure all third parties connecting to the Council's network are subject to proper controls and supervision;

- Will ensure the movement of information is in accordance with the Council's information sharing protocols (or equivalent);

- Will ensure appropriate storage of all information assets.

- Will apply the requirements of GDPR legislation, specifically compliance with the "right to be forgotten", 72hr breach disclosure to stakeholders impacted;

- Will be transparent in terms of data kept, access to that data, retention of that data, sharing and disclosure of that data.

Authorisation

- Will ensure that all staff accessing data, information and ICT systems have correct authorisation and that this is a requirement as part of their duties to the Council and its customers;

- Will maintain an accurate record of employees through well run Joiner and Leaver processes thus ensuring that only current employees have access to Council ICT systems and resources. The responsibility for notifying changes promptly to the ICT Service Providers rests with Line Managers within each Directorate to ensure that the required notice is given and the appropriate forms completed and submitted;

- Will ensure all System Owners / Information Asset Owners and the Data Controller maintain user access within all of the Council’s business systems to correspond with accurate records of who is authorised to use these systems;

- Will ensure Information Asset Owners approve data sharing with partners, have in place the appropriate Information Sharing Agreements, will undertake Privacy Impact Assessments when and where needed for business process changes, will obtain appropriate consent for the use of all data assets, will publish Fair Processing Notices when and where required, will respond to Subject Access and FOI requests and will undertake risk assessments of new processes to ensure appropriate protection and security mechanisms have been put in place;

- Will ensure appropriate control mechanisms for the authorisation and execution of password resets.

Confidentiality

- Will ensure that all staff are made aware of the sensitivity of the data they handle and manage, either on ICT systems or paper documents, and the responsibilities this places upon them. ICT Systems and procedures must be used in ways that maintain confidentiality of data;

- Will instruct staff to maintain such confidentiality at all times including outside of the workplace.

Monitoring & Compliance

- Will undertake to monitor appropriate use of the Council’s business systems including Corporate Email and Internet use. Monitoring of staff use will be undertaken in accordance with the **Information Security & ICT Use of Equipment Policy;**

- Will undertake regular compliance monitoring and audit checks to ensure compliance with the policy;

- Will maintain systems to detect and register potential security breaches, both internal to the Council and from external sources. All such activity will be logged and investigated with appropriate measures taken in response. Serious matters may require the intervention of external enforcement agencies;

- Will commission independent checks of the Council's network security on a regular basis (e.g. Independent External & Internal Penetration Testing);

- Will undertake regular monitoring and audit checks to ensure compliance with the Council's information sharing protocols or equivalent;

- Will ensure Major Incident processes are in place for the handling of all major ICT and ICT Security incidents;

- Will investigate any serious security incidents and adjust policy and procedure where this is deemed necessary;

- Will publish transparently polices for staff to be clear what the Council monitors setting out what data is held, how long it is held for, who has access to that data and for what purpose, and approval processes required to look at the data.

ICT Systems Management / Outsourcing & Third Party Management

- Will ensure security requirements form part of the specification of any new ICT systems;

- Will ensure security requirements form part of the specification of new hardware and networking;

- Will ensure security requirements form part of the procurement specification of all ICT Contracts;

- Will continuously assess data processing and ICT Systems against the Council's defined ICT standards, and risk analysis procedures will be carried out to test and check against threats and problems. The standards and procedures will continue to develop in the light of experience and evolving best practice;

- Will ensure all relevant third parties are made aware of the Council's Security Requirements and their requirement to comply with any guidance issued by the Council (**ICT Standards Expected of Third Parties**);

- Will ensure adequate Security, PCI DSS, Data Protection GDPR and FOI provisions are included in any finalised ICT Contract;

- Will ensure all significant changes are impact assessed from a security perspective as part of formal Change Management procedures with due consideration given to back-out plans and on-going refinement of policy wherever learning points occur.

Physical Access To and the Disposal of Council Information Assets

- Will ensure appropriate physical access controls are in place at all Council premises where information assets are potentially at risk;

- Will ensure physical access is given on only a "need to basis" with such access formally recorded;

- Will ensure, when working with Third Parties, that there are contractual obligations in place which set out the Council's Information Governance expectations that apply to any contract, including compliance with relevant UK legislation, obligations on the safe secure transfer, storage and handback of all assets, sharing restrictions, and security expectations in the operation of any services on behalf of the Council;

- Will ensure all information and ICT assets are disposed of in an appropriate way in accordance with best practise, Council Policy and current legislation.

Controls against Malicious Software

- Will ensure appropriate protection measures are in place to guard against malicious software attacks (including Anti Virus, Spyware, Ransomware, malicious emails etc.).

Network Management and Access Controls

- Will ensure network management and access controls are in place and monitored to protect the Council's network from malicious attack or unauthorised access;

- Will ensure the network is proactively monitored for capacity and security issues;

- Will ensure appropriate documentation is maintained for all of the critical components of the network maintaining connectivity to the Council and its authorised third parties to ensure timely recovery of systems;

- Will maintain an accurate network map;

- Will subject the network to regular penetration vulnerability tests;

- Will seek to protect the integrity of the network including adherence to the PSN Code of Connection standard for PSN operation;

- Will seek to protect all third parties connected to the Council's network through appropriate security mechanisms;

- Will provide separate secure controlled Guest Wi-Fi access for visitors as and when required;

- Will ensure the Council maintains necessary compliance standards to obtain and maintain network connectivity to the NHS N3/HSCN national networks;

Mobile Computing and Tele-working

- Will undertake to implement appropriate controls specifically to protect information and ICT assets used in a Mobile working or Tele working environment;

- Will ensure only corporately approved applications are used on mobile Devices;

- Will ensure Mobile Devices can be wiped upon loss or theft if needed;

- Will ensure mobile devices are protected by encryption and Virus/Malware scanning;

- Will ensure the Councils systems are protected against the use of personal equipment.

Systems Development and Maintenance

- Will ensure all development is subject to proper documentation and specification to allow the recovery and maintenance of both Critical and Important business system;

- Will ensure all key configuration information is recorded or recoverable in any key components of the Council's ICT Infrastructure (noting this duty may be discharged by Third Party Outsourcing and Managed Service organisations as a contracted requirement of them).

E-Services

- Will ensure proper authentication of all users accessing electronic services and/or submitting electronic transactions to the Council;

- Will ensure digital certificates and signatures are used to safeguard transactions wherever this is necessary including migration to new SHA2 Standards (and any future standards change);

- Will ensure browsers are maintained to security levels necessary for secure transactions (SSL and TLS version levels);

- Will ensure industry standards are followed and procedures revised as a when necessary (e.g. PCI-DSS);

- Will ensure appropriate use of encryption to protect key data (e.g. credit card/banking card data);

- Will consider protection within the design of Web based systems implemented as part of channel shift to minimise the threats to services from emerging targeted attacks (e.g. Denial of Service attacks, hacking, Phishing etc.);

- Will adopt the Government standard "Secure Email Blueprint" to ensure the transmission of email securely from standard council email accounts. Will look to "force TLS" between Public Sector Partners to further enhance security wherever this is feasible.

Business Continuity & Disaster Recovery

- Recognises its important role within the supplier chain and is committed to ensuring appropriate business continuity measures and disaster contingency arrangements are in place to ensure the ongoing viability of Council operations;

- Will use disaster recovery mechanisms to protect key ICT systems in accordance with industry best practise and will subject these mechanisms to regular testing;

- Will undertake to test business continuity procedures to ensure plans are accurate and have been properly maintained;

- Will ensure Business Continuity Plans and Disaster Recovery procedures are reviewed and revised in light of learning points from incidents and after any major risk change to ensure the on-going appropriateness of such arrangements;

- Will ensure Services rotate laptops taken to home overnight so as to be able to sustain a minimum service level in the event of a catastrophic event (e.g. Fire/Flood).

Cyber Crime & Cyber Fraud

- Consider the inclusion of appropriate Council insurance to safeguard the Council's interests in the event of Cyber Crime, Cyber Fraud or Cyber related incidents;

- Will ensure the Council co-operates fully with all organisations involved in the investigation of Cyber Crime, Cyber Fraud or Cyber related incidents (e.g. National Cyber Security Centre; Police, ICO etc.).

- Will ensure the timely reporting of all Cyber incidents as appropriate to the relevant national bodies in a timely manner including:

    - Directorate of Security and Intelligence (DSI) Secretariat.
    - Information Commissioner's Office
    - GovCertUK
    - South East Government WARP (SEGWARP)
    - Comsec Incident Notification Reporting and Alerting Scheme (CINRAS)
    - Thames Valley Police
    - Department of Health
    - Health & Social Care Information Centre
    - National Cyber Security Centre (NCSC)

- Will ensure Cyber Security and Cyber Crime awareness training is promoted to all Staff and Councillors to help manage the increasing Cyber based threat.

POLICY STATEMENT SIGN-UP

Council Managing Director

As the Chief Executive of Reading Borough Council I hereby give executive support (on behalf of the Council's Corporate Management Team) to the implementation and enforcement of Information Security and Information Governance policies and procedures to be adhered to by all employees and contracted organisations working as recognised agents of the Council.

Signed ……………………………………………….. Date:
(Peter Sloman)

Leader of the Council

I, on behalf of the Councillors of Reading Borough Council, support this policy statement and security policies referenced and will undertake to ensure Councillor's comply with the policies.

Signed ……………………………………………….. Date:
(Cllr Jason Brock)

Corporate Directors

We, the Corporate Directors of Reading Borough Council, support the introduction of this policy statement and security policies and will undertake to achieve compliance within our Directorates and Services.

Signed ……………………………………………….. (DR) Date:
(Jackie Yates & Section 151 Officer)

Signed ……………………………………………….. (DENS) Date:
(Frances Martin)

Signed ……………………………………………….. (DACHS) Date:
(Seona Douglas)

Signed ……………………………………………….. (BFfC) Date:
(Tony Kildare)

Other Significant Officers:

We, as other Significant Governance roles within Reading Borough Council, support this policy statement and referenced security policies and will undertake to achieve compliance within our Directorates and Services.

Signed ……………………………………………….. (DR) Date:
(Isabel Edgar Briancon) Acting Assistant Director of Customer Services & Transformation (Including Policy)

Signed ……………………………………………….. (DR) Date:
(Chris Brooks) Assistant Director of Legal and Democratic Services
Senior Information Risk Officer (SIRO) & Monitoring Officer

Signed ……………………………………………….. (DR) Date:
(Shella Smith) Assistant Director of HR & Organisational Development

Signed ……………………………………………….. (DR) Date:
(Paul Harrington – Head of Internal Audit)

Signed ………………………………………………… (DR) Date:
(Ricky Gill) Information Governance Officer - Data Protection Mgr Role)

Signed ……………………………………………….. (DACHS) Date:
(Jayne Rigg) Caldicott Guardian Role

Reading Borough Council
Working better with you

ICT Managed Services Outsourced Contractor

As the significant ICT Managed Services Outsourced Contractor to the Council we recognise this policy statement and referenced policies and will ensure our staff will comply with the policy whilst working on behalf of the Council.

Signed ………………………………………………….. Date:
(Graham Wood – Acting Client Services Director Northgate Public Services Ltd)

End of Document