Appendix 1 – ICT Policy Updates 2019-20 Full Updates List

This Appendix document is to be read in conjunction with the Report :

ICT Security Policy Set Updates 2019-20.

ICT Policies/Guidelines reviewed that required changes are:

1) ICT Policy Statement
2) ICT Use and Information Security Policy
3) ICT Golden Rules (Guideline Summary)
4) ICT Standards Expected of Third Parties
5) ICT Information Risk Management Document Marking Policy
6) ICT Email Monitoring Policy (New for GDPR)
7) ICT Internet Monitoring Policy (New for GDPR)
8) ICT Removable Electronic Media Policy

ICT Policies reviewed that required no changes are:

9) ICT Camera and Video Usage Policy
10) ICT Controls for Carriage and Storage of Hardcopy Documents
11) ICT GlassCubes Acceptable Use Policy Changes
12) ICT Huddle Acceptable Use Policy
13) ICT PCI-DSS Personal Commitment Policy
14) ICT PSN Personal Commitment Statement

Amendments to the Policies and Guidelines that follow are flagged in Blue.

Note:

1) Each change is cross referenced to the actual position in the relevant policy/ guideline document.
2) The order of document changes that now appear are as appears 1-8 above.

ICT Security Policy Statement

Change No	Section	Change
1	Document Control	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.
2	Approvals & Circulation	All revisions agreed by the Corporate Information Governance Board
3	Introduction	**THIS POLICY STATEMENT SUPERSEDES ALL PREVIOUS STATEMENTS MADE BEFORE April 2019**
4		The Information Commissioner can impose fines of up to £20m without appeal
5		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.
6		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.
7	Objectives	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 in the **ICT Security Golden Rules** guidance note) which is a joint agreement incorporated into contracts of employment and contracts for services.
8		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.
9	Information Management	Recognises the need to comply with all relevant UK Legislation (including the Data Protection Act 2018 – incorporating the 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;
10	Corporate Processes & Governance	Have set up a Corporate Information Governance Board Chaired by the Senior Information Risk Officer (SIRO) which is charged with the implementation and on-going review of the Council's ICT Security Procedures and ICT security incident recording to ensure procedures are refined and Incidents are recorded, investigated, and remedial

		measures put in place as necessary;
11	Corporate Processes & Governance (contd.)	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;
12		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;
13		Will provide appropriate professional training for key security roles (SRIO, Data protection Manager, IT Security Manager, Information Asset Owners, Caldicott Guardian);
14		Will undertake regular independent Network / Server / Desktop and Smartphone vulnerability assessments and undertake associated remedial action to mitigate any risks identified;
15		Will ensure processes are in place for on-boarding/off-boarding of all categories of workers;
16		Will ensure proper training and induction of all staff including Assistant Directors in the appropriate use of ICT and data protection compliance within the Council, including Information Governance responsibilities;
17		Will ensure all staff are aware of their Personal Commitment responsibilities when accessing PSN services and where necessary have been appropriately security checked to access such services;
18		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;
19		Will ensure appropriate data retention policies are applied appropriately to Council data assets;
20		Will ensure banking processes are appropriately authorised and overseen by Finance and PCI DSS compliance is maintained on any new arrangements entered into.
21	Legislative References	The Data Protection Act 2018 *(as revised by GDPR May 2018);
22		NIS Regulations (The Network and Information Systems 2018); Privacy & Electronic Communications Regulations (2018).
23	Local Policy References	Data Protection Policy (including Subject Access Request Procedures);
24		Breach Management Policy;
25		Internet Monitoring Policy;
26		Email Monitoring Policy.
27	Responsibility	Will ensure the roles of SIRO, Data Protection Manager, IT Security Manager, Caldicott Guardian and Information Asset Owners and Data Processors are allocated and those Information Governance responsibilities discharged appropriately throughout Council Processes;
28		A quick reference **ICT Golden Rules** Guidance Note will be made available to summarise key information for all employees and councillors to aid compliance;
29		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.

30	Council Responsibility (Contd)	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;
31		Will undertake to review and update (whenever necessary but as a minimum annually), this document, the **Information Security & ICT Use of Equipment Policy, ICT Golden Rules a**nd 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;
32		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;
33		Will ensure Major Incident Plans are in place to protect the Council from foreseeable threats (including those emerging from the Cyber landscape).
34		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;
35	Integrity of Information	Will consider all data to be key assets of the Council and will manage them as such;
36		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;
37		Will ensure its core case management systems are updated in a timely manner to reflect changes;
38		Will ensure the accuracy, quality, and appropriate retention of the data held in its case management systems;
39		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.
40	Access To Information	Will apply the requirements of GDPR legislation, specifically compliance with the “right to be forgotten”, 72hr breach disclosure to stakeholders impacted;
41		Will be transparent in terms of data kept, access to that data, retention of that data, sharing and disclosure of that data.
42	Authorisation	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;
43	Monitoring & Compliance	Will publish transparently; polices setting out what the Council

		monitors, 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.
44	ICT Systems Management, Outsourcing & Third Parties	Will ensure adequate Security, PCI DSS, Data Protection GDPR and FOI provisions are included in any finalised ICT Contract;
45	Physical Access To and the Disposal of Council Information Assets	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;
46	Network Management & Access Controls	Will ensure the Council maintains necessary compliance standards to obtain and maintain network connectivity to the NHS N3/HSCN national networks;
47	Mobile Working and Tele-Working	Will ensure only corporately approved applications are used on mobile devices;
48		Will ensure mobile devices can be wiped upon loss or theft if needed;
49		Will ensure mobile devices are protected by encryption and Virus/Malware scanning;
50	E-Services	Will adopt the Government standard "Secure Email Blueprint" to ensure the transmission of email securely from standard Council email accounts. Will look to force encryption for email delivery between Public Sector Partners to further enhance security wherever this is feasible.
51	Business Continuity & Disaster Recovery	Will ensure Services rotate laptops taken home overnight so as to be able to sustain a minimum service level in the event of a catastrophic event (e.g. Fire/Flood).
52	Cyber Crime and Cyber Fraud	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.).
53		Will ensure the timely reporting of all Cyber incidents as appropriate to the relevant national bodies in a timely manner including: • National Cyber Security Centre (NCSC);
54		Will ensure cyber security and cyber- crime awareness training is promoted to all Staff and Councillors to help manage the increasing Cyber threat.
56	Policy Statement Signup	Adjusted for current Senior Management , Political and ICT Managed Service Partners Names

ICT Use and Information Security Policy

Change No	Section	Change
57	Document Control	Updated for GDPR, Data Retention, Closedown desktops, GCSX email, Signatures, File sharing sites, Transparency Monitoring, Data Retention, smartphones, PCI, Cyber Security, Printing.
58	Document References	Data Protection Act (GDPR) 2018
59		The Code of Conduct March 1999
60		ICT Security Policy Statement Apr 2019
61		ICT Information Risk Management Document Marking Policy Apr 2019
62		ICT Standards Expected of Third Parties Policy Apr 2019
63		ICT Camera and Video Usage Policy Apr 2019
64		ICT Huddle Acceptable Use Policy Apr 2019
65		ICT Removable Electronic Media Policy Apr 2019
66		ICT GCSX (PSN) Personal Commitment Policy Apr 2019
67		ICT PCI DSS Personal Commitment Policy Apr 2019
68		ICT Controls for Storage & Carriage of Hardcopy Documentation (Guidelines) Apr 2019
69		ICT Email Monitoring Policy Apr 2019
70		ICT Internet Monitoring Policy Apr 2019
71	Glossary of Terms	ISO27001/2013 Standard for Information Security Management Systems.
72		NCSC -The National Cyber Security Centre.
73		Cyber Security Essentials (Plus) - Standards for Cyber Security set by NCSC.
74		NCSC Cloud Security Principles - Security principles set by NCSC for secure Cloud delivery.
75		ISO20000 (ITIL) - An ICT delivery Standard (IT Infrastructure Library - ITIL) published by International Standardisation Organisation.
76		CSA - Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud computing and to provide education on the uses of Cloud Computing to help secure all other forms of computing.
77		CSA STAR - CSA STAR Certification is a unique new scheme developed to address specific issues relating to cloud security as an enhancement to ISO 27001.
78		CSA CCM 3 - CSA Cloud Controls Matrix
79		GDPR - European General Data Protection Regulations – a major revision to the Data Protection Act which introduces new obligations and fine structures up to E20m and which came into effect May 2018. Led to revision of the UK Data Protection Act 2018.
80		Secure Email Blueprint - A new standard for secure Public Sector email delivery that will replace GCSX email by 31.03.2019. Using a combination of DMARC, DKIM, SPF, Transport Layer Security (TLS) standards to deliver email securely and stops external parties "spoofing" Council email. Sending email within the Public Sector will be secure by the use of TLS encryption.
81	Executive Summary	Should this not be achieved the Council's operations and customers can be put at risk (including the safety of individuals, loss of financial

		information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner with fines of up to E10m for technical breaches and E20m for bad information breaches following the GDPR revision of the Data Protection Act in May 2018).
82	2	All staff and councillors should consider the sensitivity of the information they handle (with personal and sensitive information about vulnerable people being the most important) especially in context with compliance with the Data Protection Act GDPR revision that introduced new categories of Sensitive Personal Data from May 2018 (e.g. IP addresses, Biometric data etc);
83	2	All staff and councillors will protect that information in proportion to that sensitivity by applying this policy and ensuring that information, whatever it's format, should be secured by physical means (such as locking paperwork away) or by using approved electronic means (such as only using Council IT encrypted laptop and smartphone equipment);
84	2	All staff and councillors will be responsible for the protection of their login and passwords and will not share these;
85	2	All staff and councillors will conduct their business operations in a sensible low risk manner aware of the continuing cyber security threat (be careful when opening emails and documents from external sources or visiting Internet sites);
86	4	Any breaches of security (non-compliance with this Policy) must be reported in accordance with the Council's Security Incident process by logging a Security Incident Call with the ICT Service Desk (Ext 72861) - see Appendix 4. This is to safeguard the Council and limit potential damage from information loss and to ensure appropriate notification of all relevant persons/organisations. Any data breaches must be reported and handled in accordance with the Council's Breach Management Policy.
87	Introduction 7	Such Policy and Guidenlines **must** be recognised by Staff and Councillors at all levels (including the Staff of Arm's Length Companies Wholly Owned by the Council) who must ensure they are applied at all times. Any breach of this Policy may result in disciplinary action being taken under the respective organisations disciplinary procedures or in the case of Councillors the Member Code of Conduct. In the case of Staff, where a serious breach of Policy has occurred, this may be considered Gross Misconduct which could result in dismissal from employment.
88	9	Any breaches of security (non-compliance with this Policy), however minor, must be reported to Northgate Service Desk (Ext 72861), line managers, the Council's Senior Information Risk Owner (Legal), and the ICT Manager in Corporate ICT Services, in accordance with the Council's Security Incident Management Policy and in the case of Data Incidents to the Council's Data Protection Manager using the Information Security Incident Reporting form (see Appendix 4) to

		record the incident at the earliest opportunity. Referrals may be also made to the Chief Auditor and the Assistant Director of HR & Organisational Development for further investigation.
89	Policy Statement 4	It is the policy of the Council to ensure that all information systems operated by the Council are secure systems, which must aspire to comply with the requirements of the Data Protection Act & GDPR Revision, the Computer Misuse Act and, at the level of principles, aspire to the International Standard for Information Security ISO27001/2013.
90	11	All employees and councillors are responsible for ensuring that they understand and abide by these procedures and their contents. All persons are expected to behave and act professionally at all times, and are responsible for their actions including the actions of anyone logged in as them. Failure by any employee of the Council (or any arms-length company of the Council) to abide by the contents of this document will be viewed as a serious matter and may result in disciplinary action. Failure by any councillor of the Council to abide by the contents of this document could result in action being taken in accordance with the Member Code of Conduct. CICTS will hold the Security Officer role as defined within standard ISO27001/2013 (formerly BS7799) although responsibilities may be delegated. This role will operate in conjunction with the Council's Senior Information Risk Officer (SIRO). The implementation of this policy is important to maintain and demonstrate the integrity and security of the Council's dealings with our customers, partners and other members of the community.
91	12	The Council's ICT Systems are treated as business systems and are monitored accordingly for security compliance. Any concessions for personal use are only granted on the basis of reasonable behaviour and usage that does not interfere with working, noting the concession can be withdrawn at any time, and should not be taken as a guarantee such facilities will always be available and any activities are always undertaken at the individuals own risk. Any personal activity must never expose the Council to any consequential liability, risk, Financial or reputation loss. Namely, the Workplace **must not** be considered an extension of any home personal IT environment.
92	12	It is the policy of the Council to ensure:

		• Use of Cloud based systems comply with Data Protection requirements (including any post Brexit data hosting compliance requirements).
93	15	The Information Security policy, together with the following documents, comprise the key policy and process elements of the Information Management Security System: • ICT Email Monitoring Policy • ICT Internet Monitoring Policy
94	Goals of the Policy 18	To comply with legislation, examples of which include; • Data Protection Act 2018
95	Responsibilities 25	The Council's Caldicott Guardian will ensure compliance with Information Governance from a Social Services perspective.
96	Removable Media 50	If you need to work on Council information at home or at a remote location, the Council secure VPN system must be used from a Council-issued computer, tablet and smartphone to safeguard data, unless in exceptional or temporary circumstances with the prior consent of an Assistant Director. Council laptop devices connecting across Open Public Wifi Access, or Public Wifi where the SID and Password Key are on open display must be protected by additional security (e.g. TLS, IPSEC VPN) to protect the traffic.
97	Mobile phones 55	Staff and Councillors issued with mobile phones, Smartphones, Tablets or other Personal Digital equipment are responsible for its safekeeping and security.
98	64	Council-issued Mobile phones, Tablets, Smartphones and PDA's are provided for work-related purposes.
99	Mobile Telephones, Smart Phones & Tablets, & Faxes 74	Email with confidential personal information must not be sent from mobile devices unless the device has appropriate security measures (e.g. encryption). Special care should be taken in the operation of Faxes, (as there is no control over documents printed out at the other end) and their usage should be avoided if practically possible. Council

		mobile devices connecting across Open Public Wifi Access, or Public Wifi where the SID and Password Key are on open display must be protected by additional security (e.g. TLS, IPSEC VPN) to protect the traffic.
100	Passwords 76	In all cases any passwords given to you personally are for your use only. Keep Passwords safe and you are responsible for your actions and anyone logged in as you. Passwords should not be written down in an insecure location or given to others to use under **any** circumstances. This includes your manager or Political Group Leader (if you are a Councillor). If your Manager or Political Group Leader needs access to your computer, for example if you are off sick, they must contact the ICT Service Desk to request managerial access to your computer. You should also register a "Safeword" to assist with any Password reset which will avoid needing further identity checks (contact the ServiceDesk Ext 72861 for advice on the "Safeword" set up process).
101	78	Do not use family or pet names and if at all possible try not to use proper words. This makes the accidental discovery of a password more difficult. Avoid the use of personal passwords used in your private home environment.
102	79	Your password must be changed if you feel it has been compromised. You should not choose a password that you have previously used.
103	Internet chat Facilities and Social Networking 107	Individuals may access and use approved chat rooms, discussion group's bulletin boards and social networking sites, but must not post comments that identify or indicate such views to be those of the Council unless authorised to do so by the Council's Strategic Communications Manager. Social Media is now a common channel customers expect to communicate over. When using Social Media for Business Purposes you are asked at all times to give proper consideration to the fact that you are making statements on behalf of the Council, that you should have the appropriate knowledge, authority and clearance to make such statements, and have considered your options for statement retraction should this ever prove to be necessary. Please ensure any accounts entered into are properly recorded within your service area and are therefore transferable to other staff in the event that you leave the authority. If you want to use the Council concession that allows for reasonable access to Social

		Media for occasional private means, you do so knowing the Council's systems are monitored and reported on as business systems and if you are unhappy to accept this then you should make your own separate arrangements for such access (e.g. personal private smartphone). Any personal social media access should not incur any reputational or financial liability for the Council.
104	Monitoring & Misuse 108	RBC's web filtering and monitoring software both limits what individuals may access and logs those sites that individuals access or attempt to access. If a line manager or Political Group Leader is concerned that an individual is misusing their access to the Internet they should contact the ICT Manager or HR Business Partner and make a request for the individual's usage to be investigated. There are further specific separate transparency policies dealing with the monitoring and role based access relating to staff and councillor email and internet use so staff and councillors can be clear on what is held, for how long, who can access this information. Please refer to these policy documents for further detailed clarification.
105	Email 112	Following adoption of the Secure Email Blueprint standard (DMARC/DKIM/SPF/TLS) both @reading.gov.uk and @brighterfuturesforchildren.org email domains transmit and receive e-mail securely to email domains within the Public Sector.
106	113	Email sent outside the Public Sector should not be considered secure. Staff should take care to ensure email addresses are selected /typed correctly to avoid miscommunication.
107	114	Any email with sensitive data or attachments please use Global Certs secure email when sending externally outside of the Public Sector to protect the contents of the email.
108	115	Sensitive email should be appropriately document marked (e.g. OFFICIAL, OFFICIAL-SENSITIVE), when sending internally or to other Public Sector Organisations who recognise the Government Document Marking Standard. It is optional to use document marking outside of the Public Sector as the recipient is not likely to understanding the scheme unless explained.
109	116	Please be careful clicking on links or attachments received in emails from external sources.

110	User Responsibilities 131	Each individual must ensure that as far as is possible no unauthorised person has access to any data held by the Council. Each person must ensure that any physical security measures are properly used. If you think a security breach has occurred please report this immediately to your Manager and the Northgate Service Desk.
111	132	Staff & Councillors will ensure they reload their computers on a regular basis to ensure patches applied are activated to protect their device.
112	PCI DSS 163	The use of personal Smartphone devices that could record or photograph cardholder data should be controlled where payments are taken.
113	Use of Skype 196	Currently Skype is only allowed on a bookable laptop requested via the Northgate ServiceDesk (Ext 72861). This laptop has to connect over the Council's GUEST Wifi network. This will be relaxed for Skype for Business/Teams upon the roll-out of Microsoft Office 365 and will then be allowable across the corporate network.
114	Computer User Security Responsibilities 208	1.You will have a log on account which is unique to you and which you must not let anyone else use. You will reload your computer on a regular basis to activate software security patches.
115	208	• Your passwords must be changed if you ever suspect it has been compromised.
116	208	• Please do not reuse passwords you use at home.
117	208	You must ensure any equipment or data losses are treated as security incidents and reported to the Northgate Service Desk (ext 72861). Under GDPR the Council has 72 hours to report to all affected stakeholders any data breach and what action has been taken to recover the position.
118	208	You will be careful not to take unnecessary risks when clicking on links or opening attachments in emails sent from external sources. If in doubt on the authenticity of an email check with your Manager or the Northgate Service desk.
119	Service Manager Responsibilities 212	You must ensure Privacy Impact Assessments (GDPR) are undertaken when your service process changes, along with the publication of Fair Processing Notices where applicable for your service.
120	Chief Executive, Directors and	Ensure the following key roles are in place and adequately trained to

	Assistant Director Security Responsibilities 214	discharge their duties: Senior Information Risk Officer (SIRO) Data Protection Manager ICT Security Manager Caldicott Guardian Information Asset Owners.
121	214	Ensure Information Governance responsibilities are set out in Job Descriptions so all staff know their responsibilities and roles.
122	214	Ensure sound Information Governance Processes are embedded across the Council and Information Assets are appropriately protected.
123	214	Ensure appropriate Information Governance and Security Induction training and guidance is in place for Councillors and staff.
124	Appendix 3 - Related Policies & Documentation	• ICT Email Monitoring Policy • ICT Internet Monitoring Policy • ICT Huddle Acceptable Use Policy • RBC Breach Management Procedure
125	21.2 Legal References	• Data Protection Act 2018 (GDPR Revision)
126	Appendix 4 Security Incidents	Information Security Incidents should be reported in accordance with the Council's Security Incident Policy which classifies the type of security incident and ensures appropriate notification of relevant parties including CICTS, Legal SIRO, Data Protection Manager and external organisations set out in the Council's Major Incident & Security Incident Process.

ICT Golden Rules (Guidelines)

Change No	Section	Change
127	Golden Rules 1	You are responsible for all actions logged against your own Login/password. Please do not share your passwords and remember to lock your PC when away from your desk. Be professional in your actions at all times. **HINT!** – The Windows key plus the L key locks your PC quickly. *(Ref: ICT Use & Information Security Policy).*
128	2	Always use strong passwords at least 9 characters in length with a complex format. Do not mix business and personal use passwords and always change your password a.s.a.p if you think it has been compromised. **HINT!** – check the strength of your password at: https://howsecureismypassword.net/ **HINT!** – Ctrl Alt Delete will allow you to change your Windows password. *(Ref: ICT Security Policy Statement, ICT Use & Information Security Policy).*
129	3	If you have forgotten your password please call the Northgate Service Desk (0118 9372861 or ext 72861) for PC's and Laptops, or CICTS (0118 9373911 or ext 73911) for smartphones/tablets. **HINT!** – With a smartphone or tablet please call before you get to the last try and it will stop your device being wiped. *(Ref: ICT Use & Information Security Policy).*
130	4	Be careful to select the correct email address from the Global Address List when sending emails. **HINT!** – External/third party email addresses have a Globe symbol against them in the Global Address List.
131	5	Avoid clicking on links or opening documents contained in external emails unless you are sure the email is genuine and you know the sender. **HINT!** – a red warning banner shows at the top of all external incoming emails.
132	6	Use document marking for emails and personal/sensitive documents. If a document is marked as OFFICIAL-SENSITIVE and is being sent externally please ensure that it is shared securely. **HINT!** – If in doubt, use Global Certs secure email triggered by [Secure] at the start of the subject line of your email. *(Ref: ICT Use & Information Security Policy & Information Risk Management Document Marking Policy).*
133	7	Please ensure you fully shutdown your PC or Laptop at the end of the day. **HINT!** – Ctrl + Alt + Del and then selecting shutdown (bottom right) does this quickly.

		(Ref: ICT Use & Information Security Policy).
134	8	Be aware that callers/letters/Invoices may not always be genuine and could be rogue Phishing or Social Engineering exercises to obtain personal information, commit fraud or illegally gain access to the Council's systems. Never be frightened to challenge the identity of a caller or question the validity of a document especially at peak work times. *(Ref: ICT Use & Information Security Policy)*
135	9	In the event of potential malware activation immediately power down your laptop/PC by pressing the power button and pull any network lead out. Then please contact the Northgate ServiceDesk (Ext 72861) to alert them. **HINT!** – Pressing the power button ensures Wifi/network disconnection. *(Ref ICT Use & Information Security Policy).*
136	10	You are obliged to report any significant ICT security incidents to the IT Service Desk (Ext 72861) as soon as you become aware of something. Under the new Data Protection 2018 GDPR regulations incidents must be reported to the Information Commissioners Office within 72 hours. **HINT!** – Have the Northgate ServiceDesk Number (0118 9372861) in your mobile phone in case need to report a security incident when away from your desk. *(Ref: ICT Use & Information Security Policy,* *RBC Breach Management Procedure).*
137	Further Non-IT Policy References	Further Non-IT Policy References: RBC Breach Management Procedure RBC Data Protection Policy RBC Social Media Policy
138	Contacts	Data Protection Advice – Ricky Gill Data Protection Officer (Ext 73306)
139	Helpful Contacts	Northgate IT Service Desk (Ext 72861), Email: ps_servicedesk@northgateps.com

ICT Standards Expected of Third Parties

Change No	Section	Change
140	Document Control	Reviewed GDPR, PCI DSS, Cloud, Secure Email Blueprint Standard, Cyber Security Major Incident Plans, Organisational Changes.
141		All revisions approved by the Corporate Information Governance Programme Board will be notified to third party organisations as recorded issued to this document
142	Legislative compliance References 3.3	• The Data Protection Act 2018 (GDPR Revision)
143	3.4	**Data Protection Act 2018 - GDPR Compliance** Reading Borough Council will expect Third Parties to comply with the Data Protection Act 2018 - General Data Protection Revisions (GDPR) and have embedded the six key security principles into operations and data processing: • Maintain Lawfulness, **fairness** and **transparency**. (**Transparency**: Tell the subject what data processing will be done). • **Purpose** limitations. • Ensure Data minimisation. • **Ensure Data Accuracy**. • Maintain Storage limitations. • **Maintain Integrity** and **confidentiality**. **For the avoidance of doubt this means:** **Lawful, Fair and Transparent** Transparency: explain to the data subject that data is being captured and what that data is, why that data is being captured, and by whom, and what will happen to that data. Fair: what is processed must match up to how it has been described. Lawful: processing must meet the tests described in GDPR. **Purpose Limitations** Personal data may only be collected for the specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes, i.e. data can only be used for the specific purpose the data subject has been made aware of and no other, without further consent. **Data Minimisation** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, i.e. no more than the minimum amount of data should be kept for specific processing.

		Data Accuracy Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Ideally, data should be stored in a way that allows a data subject to update the data themselves **Storage Limitations** Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary, i.e. data no longer required should be removed. **Integrity and Confidentiality** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. GDPR recommends encryption of personal data and privacy by design process **Further to this the Council would expect:** • Processing of data only in accordance with what has been agreed with the Council; • No sharing of data unless agreed and authorised by the Council; • Systems are appropriately protected from Cyber threats; • Appropriate consideration is given to the transfer, storage, and hand back of data so as to appropriately protect the Council's Information Assets at all points; • Work with the Council to ensure Appropriate Fair processing notices to be in place where applicable; • Work with the Council to ensure Privacy Impact Assessments are in place where any significant changes in service delivery or processes have taken place; • Action any "right to be forgotten" requests where appropriate; • Comply with 72hr notification of all interested parties following breach; • Ensure staff are appropriately trained and supervised in their operations to ensure they understand and comply with their respective Information Governance roles.
144	Payment Card Industry Security Standards 3.5	Reading Borough Council will ***expect*** third parties to comply with PCI DSS Standards when delivering any banking and credit card payment transaction services, and where the third party is not delivering these services they **must** not compromise the Council's PCI DSS Compliance (whether delivered directly by the Council or other third parties). This must include appropriate best practice end to end secure encryption of banking and credit card data in both the transmission and secure storage of any banking and

		credit card data. Only operate services over PCI DSS secure Wifi, secure Wide Area Networks and secure Local Area Networks. Only operate services over PCI DSS secure telephony systems. Appropriate training and supervision of staff including the restriction of Smartphones usage (to protect against photographs/video recording/voice recording of banking data) in the delivery of banking and credit card payment taking services.
145	Business Continuity & Disaster Recovery 3.14	Typically disaster recovery mechanisms should include: • Major Incident Plans to deal with foreseeable events especially in the emerging Cyber Security landscape.
146	Cloud Services 3.15	**Cloud Services.** As Cloud Service delivery becomes increasingly the normal, Reading Borough Council ***expects*** the Third Party to have used industry best practice standards to manage the risks associated with Cloud Hosting to safeguard the Council's services and ensure appropriate ease of transition at the end of any contracts. The Third party will ensure: • Appropriate known geographic hosting of data so as to be compliant with UK law; • Hosting in appropriate secure regulated Data Centres to Tier 2 or Tier 3 subject to the availability profile the service needs (Tier 2: Guaranteeing 99.741% availability, Tier 3: Guaranteeing 99.982% availability). • Service provisioning will comply with all UK ICT Legislation including GDPR; • Adherence to ISO27001 and ISO 27002 Security Standards as revised from time to time; • Adherence to Cloud Standards CSA STAR, CSA CCM 3, and NCSC Cloud Security Principles; • Adherence to Industry Best Practice for Cloud delivery as set out in: ▪ The principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications; ▪ The guidance issued by the Centre for Protection of National Infrastructure on Risk Management at

		https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets; ▪ The National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection; ▪ The government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice; ▪ The security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles ; • Cyber Security https://www.ncsc.gov.uk/guidance/10-steps-cyber-security. • Disaster Recovery Provisions to underpin the Business Continuity required by the Council; • Transparent charging which meets the Council's operational service availability requirements (including any evening, weekend provisions or further special periods e.g. Bank Holiday/Christmas etc ; • Appropriate provisioned support for the secure transition of Council data at the end of any contracted period to new arrangements at pre-agreed known rate card charges which the Third Party will reasonably resource.
147	Operational Procedures 4.5	The Council ***expects*** the Third Party: • To train and supervise Staff in relevant Procedures and Policies
148	Operating Email Services 4.13	The Council expects the Third Party will comply with the Secure Email Blueprint standard when transmitting email on behalf of the Council to the required DMARC/DKIM/SPF and TLS standards.
149	Cyber Security 8	The Council ***expects*** all Third Parties to have considered and protected against foreseeable Cyber Security threats in line with industry best practice. The Council ***expects*** all Third Parties to have Major Incident Plans in place to deal with foreseeable Cyber Security Threats.

150	Reporting of Security Breaches 9	The Council ***must*** be informed immediately in the event of any Security Breach or major Service Outage. The Council ***expects*** all Third Parties will notify all relevant Stakeholders within 72 hrs of discovery of a data breach that that breach has happened and the action taken to recover from that position as is required by the Data Protection Act 2018. The Council ***expects*** all Third Parties to have considered insurance to protect The Council and themselves against claims resulting from Security Incidents.

ICT Information Risk Management Document Marking Policy

Change No	Section	Change
151	Document Control	Reviewed for GCSX Retirement & Data Protection Act 2018
152	Introduction 1.0	• All information assets (paper, files, electronic media, emails or other) to be processed by Reading Borough Council (the Council), shall be protectively marked in accordance with the sensitivity of their content, following the requirements of HMG Security Policy Framework, and in compliance with standards laid down by the Digital Cabinet Office. The protective marking of an information asset provides people with information on:-
153	Legal 4.1	• The Data Protection Act 2018 GDPR Revision;
154	Transmitting Protectively Marked Material 12.2	Following adoption of the Secure Email Blueprint Standard across the Public Sector, email transmitted to other Public Sector Organisations from @reading.gov.uk and @brighterfuturesforchildren.org email accounts will be securely protected by Transport Layer Security (TLS) encryption. Within the Public Sector this will protect email to both **OFFICIAL** and **OFFICIAL-SENSITIVE** Levels (but note Global Certs secure email can still be used if deemed necessary). Global Certs secure email must be used when sending to any other external address outside of the Public Sector where the content or attachments are deemed to be sensitive.
155	Storage and Security of Protectively Marked Material 14.4	For the purposes of storing and processing electronic **OFFICIAL-SENSITIVE** and **OFFICIAL** data between Central Government and other Councils, the Council has adopted the secure email blueprint or other security systems deemed appropriate as set out by HM Government.
156	14.5	The Council shall protect the data by installing or adapting existing systems, with reference to national standards for Information Security and the provisions of the Data Protection Act 2018, as well as current policies and standards adopted by the Council.
157	Additional Control Measures 18.2	a. Use of Secure Email Systems (e.g. TLS & Global Certs);
158	Security Incident Reporting 19.1	The Council is obligated to review and on occasions externally report security incidents relating to Protectively Marked Documents and emails. This includes, but is not restricted to: • Physical loss of a printed protectively marked document or email; • Inappropriate sending of **OFFICIAL-SENSITIVE** documents and emails across unsecured email; • Inappropriate sending of **OFFICIAL** documents and email across unsecured email;
159	Appendix B	**External Internet Email to Public Sector:** Use @reading.gov.uk /@Brighterfutures.org email (protected by TLS).

160		**External Internet Email to Others** : Use Global Certs secure email for non-public sector recipients if content sensitive.

ICT Email Monitoring Policy (New Policy)

161	ICT Email Monitoring Policy	New Policy therefore changes not individually listed

ICT Internet Monitoring Policy (New Policy)

162	New Internet Monitoring Policy	New Policy therefore changes not individually listed

ICT Removable Electronic Media Policy

Change No	Section	Change
163	Document Control	Revised for Data Protection Act 2018 (GDPR)
164	Scope	Removable electronic media (examples of which include USB Memory Sticks, CD's, DVD's, SD cards) can pose a significant risk of automatic fines under the Data Protection Act 2018 of up to £20m for the Council and further liability for the Individual with limited rights of appeal, if such media is lost containing Sensitive Personal Data.
165	Scope	In particular staff and councillors shall not: 1. Use unencrypted removable electronic media to hold personal or sensitive personal data as defined under the Data Protection Act 2018:
166	Sensitive Personal Data	Sensitive Personal Data: Sensitive Personal Data is data that identifies an individual's race or origin, an individual's religion, an individual's political beliefs, an individual's sexual health, and individual's health, an individual's criminality history, an individual's financial records and any data relating to children, biometric data, and Genetic data.
167	Take All Reasonable Steps 11	Report any loss as a security incident to the Northgate Service Desk Ext 72861 at the earliest opportunity and complete the Report of Loss of Data form and return to Legal Section / SIRO. Under the Data Protection Act 2018 the Council has 72 hours to inform all stakeholders of an incident and remedial action being taken so it is imperative that any incident is immediately reported upon discovery it has happened.

End of Appendix 1