READING BOROUGH COUNCIL

REPORT BY EXECUTIVE DIRECTOR OF RESOURCES

TO:	**POLICY COMMITTEE**		
DATE:	**16 DECEMBER 2019**		
TITLE:	**ICT SECURITY POLICY SET UPDATES 2019-20**		
LEAD COUNCILLORS:	**COUNCILLOR EMBERSON**	**PORTFOLIO:**	**CORPORATE & CONSUMER SERVICES**
SERVICE:	**ALL**	**WARDS:**	**BOROUGHWIDE**
LEAD OFFICER:	**JOHN BARNFIELD**	**TEL: 0118 937**	**0118 9372860**
JOB TITLE:	**ICT TECHNOLOGY & SERVICES MANAGER**	**E-MAIL:**	**John.Barnfield@reading.gov.uk**

PURPOSE OF REPORT AND EXECUTIVE SUMMARY

1.1 To seek approval of the annual revisions to the Council's ICT Security Policies and accompanying summary guidance notes for 2019-20.

1.2 To note the ICT Policy Set consists of 13 Policy Documents, with key compliance and required behaviour practices summarised in the "ICT Golden Rules" summary document for ease of stakeholder uptake.

1.3 To note that the proposed changes represent a substantial revision of the Council's ICT Policies incorporating legislative and cyber best practice requirements and standards that have recently emerged, alongside more routine updates that are now needed. The Council could be at risk of fines and possible standards breaches if these changes are not approved and effectively communicated to Staff and Councillors. The changes (highlighted in **blue** and cross referenced to the documents concerned) are attached as Appendix 1 – ICT Policy Updates 2019-20 Full Updates List, along with the 3 key documents to be issued to Staff and Councillors as Appendix 2.1 – ICT Security Policy Statement v1.7, Appendix 2.2 – ICT Use & Information Security Policy v1.9 and Appendix 2.3 – ICT Security Golden Rules v1.9.

1.4 To note further training and briefings will be provided to Council Staff, Staff of Council wholly owned companies and Councillors as part of a wider communications plan to embed a good knowledge of the key changes across the Council as set out in 4.2.3.

1.5 To note a delegation will be sought for the Executive Director of Resources in consultation with the Lead Councillor, to approve future revisions of the ICT Policy Suite to speed up the revision release process. The Policies will apply to both the Council, the Council's wholly owned companies and to Councillors.

2. RECOMMENDED ACTION

2.1 To approve the revised ICT Policy Suite & Guidance Notes for 2019-20.

2.2 To note the communications plan for Staff and Councillors including associated briefings and training set out in 4.2.3.

2.3 To delegate future revisions of the ICT Policy Suite & Guidance Notes to the Executive Director for Resources in consultation with the Lead Councillor for Corporate and Consumer Services.

Appendices:
Appendix 1 – ICT Policy Updates 2019-20 Full Updates List;
Appendix 2.1 – ICT Security Policy Statement v1.7;
Appendix 2.2 – ICT Use & Information Security Policy v1.9;
Appendix 2.3 – ICT Security Golden Rules v1.9.

3. POLICY CONTEXT

3.1 Information Technology is a key enabler of service delivery across the Council. All staff, councillors, and partners, as part of good corporate governance, are required to understand the acceptable use constraints and operational expectations when using and working with the Council's ICT systems and infrastructure to ensure compliance with UK Legislation and safeguard the Council's operations and data from cyber-attacks.

3.2 The Data Protection Act 2018 (General Data Protection Revision – GDPR) introduced new obligations for the safe handling of data, new categories of Personal Sensitive Data (e.g. Biometric data), and significantly increased the fines that can be imposed for both non-compliance with the new legislation and data breaches, which includes the right to compensation for data subjects adversely impacted by any data breach. Organisations can now be fined up to £20m or 4% of their global turnover, whichever is the larger. The Information Commissioners Office has to date issued fines up to £183m, with potential further compensation claims by affected data subjects having been lodged. This shows a clear intent that the Information Commissioners Office is prepared to fine organisations heavily if they do not take their Information Governance and Data Protection responsibilities seriously and is likely to extend into the Public Sector in order to change behaviour.

3.3 ICT Policies are subject to annual review to ensure they remain fit for purpose, address emerging threats and reflect best practice. This in turn helps to protect service operations which rely on ICT for delivery. The threat from cyber-attack continues to grow, and there are examples of Ransomware attacks that have cost councils in excess of £2.5m to recover. Most attacks originate from poor end user behaviour, whether by clicking on internet links in emails from unknown sources, or falling victim to social engineering and Phishing attacks which obtain login credentials and passwords allowing unauthorised access to systems that result in data breaches.

3.4 ICT supports significant front line service delivery to residents and service users. Maintaining good security is critical to maintaining customer confidence and the long term sustainability and success of service delivery.

4. THE PROPOSAL

4.1 Current Position:

4.1.1 The former ICT policy suite consisted of 13 documents and one "Golden Rules" summary guidance note (which presented key compliance requirements in an easily digestible format to help uptake).

4.1.2 As a result of the Data Protection Act 2018 GDPR changes, two additional Policy documents have been added to meet the new transparency criteria required, firstly in respect of business email monitoring and secondly internet usage monitoring. The policies make clear what is monitored, why, by whom and the retention of such material that may otherwise not be obvious to the end user.

4.2 Proposal:

4.2.1 To publish a revised ICT Policy Suite comprising 13 policy's as set out below and a "Golden Rules" summary guidance note for 2019-20. The proposed full ICT Policy Suite consists of:

ICT Policy Suite:

- ICT Policy Statement;
- ICT Use & Information Security Policy;
- ICT Internet Monitoring Policy (new for GDPR);
- ICT Email Monitoring Policy (new for GDPR);
- ICT Standards Required of Third Parties;
- ICT Risk Management & Document Marking Policy;
- ICT Camera and Video Usage Policy;
- ICT Controls for Storage & Carriage of Hardcopy Documents;
- ICT GlassCubes Acceptable Use Policy;
- ICT Huddle Acceptable Use Policy;
- ICT PCIDSS Personal Commitment Policy;
- ICT PSN Personal Commitment Policy;
- ICT Removable Electronic Media Usage Policy.

Summary guidance note:

- ICT Golden Rules.

4.2.2 These Policies and Guidelines have been revised in respect of:

- Data Protection 2018 (General Data Protection Regulations)
  - Transparency Policies for Email and Intranet Monitoring,
  - Scope change to include IP Addresses & Biometric Data,
  - 72hr Incident Reporting,
  - Data Hosting restrictions;
- GCSx Secure Email Retirement;
- Changes recognising Secure Email Blueprint Standards adoption;
- Password Management (relaxation of 90 day change policy;
- Mobile Device Management;
- Cyber Security Risk Management;
- Reducing the Impact of Thefts;
- Return of Leavers IT Equipment;
- Requirement to shutdown laptops;
- Required action to take for Malware/Ransomware events;

- Restrictions sending work to Private Personal Email Accounts;
- Requirement to timely Updating of Case Management Systems;
- Requirements for Email Signatures;
- Increased controls when operating in Public Open Wifi zones;
- Limitations on use of File Sharing Sites;
- Relaxation of access to Social Media sites;
- Requirements for Data Retention compliance;
- Compliance changes for PCI DSS Bank Credit/Bank Card handling;
- Protecting Against Identify Theft;
- Printing restrictions at home;
- O365 Skype/Teams Usage;
- Increased responsibilities on Third Parties operating ICT;
- Changes in Organisational Structure and Role Responsibilities;
- Requirement for Cyber Security Induction.

Appendix 1 details the revised proposed polices with the changes highlighted in **blue**.

4.2.3 Following approval, the revised Policy Suite and summary guidelines "Golden Rules" will be issued in accordance with the communications plan which includes:

- Intranet Posting & Blog;
- Sign-posting in Staff News;
- Sign-posting via the Chief Executives Blog;
- Team Talk Managers Briefings;
- Councillor Briefings;
- Revised Induction Training;
- Important Systems Information Messages;
- New Online Training Opportunities.

4.2.4 The 3 key documents, the ICT Policy Statement, ICT Use and Information Security and ICT Golden Rules will, as part of the communications plan, be issued to Council staff, staff of Council wholly owned companies and Councillors with associated briefings and training provided to embed a good level of understanding of the key changes.

Appendix 2.1, 2.2, and 2.3 details these three key documents.

4.2.6 To speed up the issue of future amendments to these key documents it is recommended that delegated authority be granted for the Executive Director of Resources in consultation with the Lead Councillor for Corporate and Consumer Services to approve future revisions of the ICT Policy Suite and summary "Golden Rules" Guidance Notes.

4.2.7 Options for further supporting training for Cyber Security, Information Governance and Councillor specific training are under review and are expected to be delivered within existing budget provisions approved for transformation.

5. CONTRIBUTION TO STRATEGIC AIMS

5.1 The effective use of ICT is fundamental in supporting new ways of working and service transformation, which together both help the Council move to a lower cost operational model and more flexible access to services.

5.2 ICT underpins most service delivery across the Council and it is also fundamental to the continuing successful delivery of services as set out in the Corporate Plan and Service Plans.

5.3 These Policies offer further protection to the Council recognising the increased importance of ICT in delivering services securely in a modern organisation.

6. COMMUNITY ENGAGEMENT AND INFORMATION

6.1 The ICT Security Polices will support the internal Corporate Governance model of the Council and in turn the delivery of secure and efficient services to its customers.

7. EQUALITY IMPACT ASSESSMENT

7.1 The Policies set standards of working which apply regardless of disability, age, gender, religion, ethnicity, nationality, sexual orientation or first language.

8. LEGAL IMPLICATIONS

8.1 Adoption of these ICT Policies directly support compliance with all UK ICT legislation in particular the Data Protection Act 2018.

8.2 Relevant and updated ICT Policies are considered best practice essential to managing both Information Governance and Security Risks across any organisation to minimise the likelihood of fines which can be imposed now by the Information Commissioners Office at levels up to E20m or 4% of and organisations Global Turnover whichever is greatest.

9. FINANCIAL IMPLICATIONS

9.1 Revenue Implications.

9.1.1 There are no direct revenue implications arising from the approval of these Policies. Rather they seek to protect the Council from avoidable fines and ensure customer confidence in the Council and its services is maintained.

9.1.2 Fines of up to £20m or 4% of an organisations worldwide turnover can be levied by the Information Commissioners Officer (ICO) for failing to adhere to the Data Protection Act 2018 (GDPR) where serious data breaches occur. These IT Policies help to protect against the possibility of ICO fines.

9.1.3 Data Subjects are now entitled to lodge compensation claims where they have been affected by data breaches. With the PPI industry looking for its next claim opportunity, there is a strong possibility companies will move into the Data Protection compensation space. It has been reported openly in the press one organisation may have claims against it lodged of up to £500m resulting from a serious data breach affecting its customers. The associated loss of customer confidence is also likely to be reflected in reduced sales so the final cost is likely to be even higher.

9.1.4 It is not unreasonable to assume the ICO will make an example of a Public Sector organisation when the sector suffers its next serious data breach or non-compliance event with the Data Protection Act 2018 in order to force all Public Sector bodies to address any Information Governance and Data Protection weaknesses they may have.

9.1.5 Copeland District Council suffered a Cyber Ransomware event with financial consequences of £2.5m to recover. So the risks are real for Local Authorities and Security Policies and raising awareness of the threat with end users and associated Cyber Security training is necessary to mitigate these risks.

10. ENVIRONMENTAL IMPACT

10.1 None arising.

11. BACKGROUND PAPERS

11.1 None arising.

READING BOROUGH COUNCIL
REPORT TEMPLATE

FINANCIAL IMPLICATIONS

The financial implications arising from the proposals set out in this report are set out below:-

1. Revenue Implications

Use this Table in the report or as an Appendix to set out the revenue implications:

	2019/20 £000	**2020/21 £000**	**2021/22 £000**
Employee costs (see note1) Other running costs Capital financings costs			
Expenditure	0	0	0
Income from: Fees and charges (see note2) Grant funding (specify) Other income	0	0	0
Total Income	0	0	0
Net Cost(+)/saving (-)	0	0	0

2. Capital Implications

Capital Programme reference from budget book: page line	**2018/19 £000**	**2019/20 £000**	**2020/21 £000**
Proposed Capital Expenditure	0	0	0
Funded by Grant (specify) Section 106 (specify) Other services Capital Receipts/Borrowing			
Total Funding	0	0	0

3. Value for Money (VFM)

Training modules were produce by crowd funding (by other Local Authorities) and are the lowest cost of the quotes obtained.

4. Risk Assessment

There is a significant risk of fines that can be imposed by the ICO for Data Breaches or non-compliance with the Data Protection Act 2018 (GDPR). Examples of intent to fine in the Private Sector already run to an example of £183m with £500m compensation claims thought to be also lodged with two major legal companies. A similar level of fine for serious data breaches is likely at some point within the Public Sector.