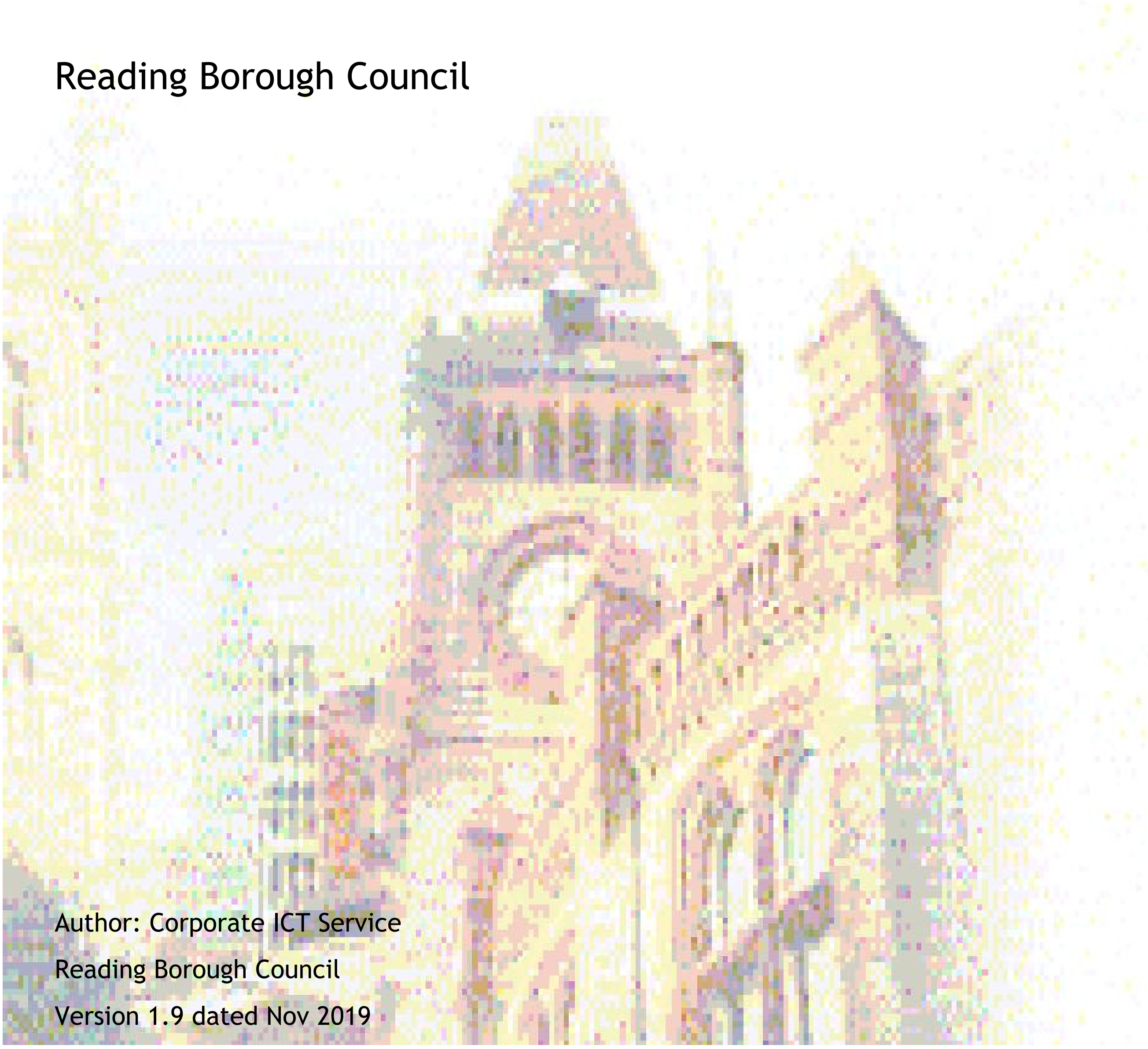
ICT Security Golden Rules

Reading Borough Council



Author: Corporate ICT Service

Reading Borough Council

Version 1.9 dated Nov 2019

ICT SECURITY GOLDEN RULES (GUIDELINES)

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).

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).

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).

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.

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.

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).

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).

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)

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).

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).

Please note these ICT Security Golden Rules are not a replacement for the Council's ICT Policies (which are published on the Council's Intranet). It remains your responsibility to be familiar with the detail of the ICT Policies, supported by further Guidelines as set out below:

Policies:

ICT Security Policy Statement

ICT Use & Information Security Policy

ICT Information Risk Management Document Marking Policy

ICT Standards Expected of Third Parties Policy

ICT Camera and Video Usage Policy

ICT Huddle Acceptable Use Policy

ICT Removable Electronic Media Usage Policy

ICT PCI DSS Personal Commitment Policy

Guidelines:

ICT Security Golden Rules (this document)

ICT Controls for Storage and Carriage of Hardcopy Documentation

Further Non-IT Policy References:

RBC Breach Management Procedure

RBC Data Protection Policy

RBC Social Media Policy

Helpful Key Contacts:

Senior Information Risk Officer (SIRO) - Chris Brooks, Assistant Director of Legal & Democratic Services, (Ext 72602)

Data Protection Advice – Ricky Gill Data Protection Officer (Ext 73306)

CICTS Security Role – John Barnfield, IT Technology & Services Manager
(Ext 72860)

Internal Audit – Anthony Kearns, Principle Auditor (IT)
(Ext 72692)

Northgate IT Service Desk (Ext 72861),
Email: ps_servicedesk@northgateps.com

CICTS Email: CorporateICT.Service@reading.gov.uk

End of Document.