Public Document Pack

CHESTERFIELD
BOROUGH COUNCIL

Please ask for Joel Hammond-Gant
Direct Line: 01246 34 5273
Fax: 01246 345252
Email: committee.services@chesterfield.gov.uk

The Chair and Members of Cabinet

Dear Councillor,

AGENDA SUPPLEMENT

Please see attached the documents for the agenda item(s) listed below for the meeting of the CABINET to be held on TUESDAY, 15 MAY 2018, the agenda for which has already been published.

11. Information Management Policy Refresh - General Data Protection Regulation (GDPR) (Pages 3 - 60)

Yours sincerely,

Local Government and Regulatory Law Manager and Monitoring Officer

This page is intentionally left blank

For publication

Information Management Policy Refresh – General Data Protection Regulation (GDPR) (GV250)

Meeting: Cabinet

Date: 15 May, 2018

Cabinet portfolio: Cabinet Member for Governance

Report by: Information Assurance Manager

For publication

1.0 Purpose of report

1.1 To advise Members of the production of updated Information management policies.

2.0 Recommendations

2.1 That Members consider the updated Information management policies.

2.2 That the proposed policies, attached at Appendix A, be approved and that the existing ICT Policy be decommissioned.

2.3 That changes to the policies be authorised after 25th May 2018 to reflect further guidance from the ICO, NCSC or other respected authorities, but that any changes will only be

implemented after consultation with relevant senior leaders, senior managers and portfolio holder(s).

3.0 Report details

3.1 The Information management policies are required to meet the forthcoming General Data Protection Regulation (GDPR). The updated policies provide the necessary controls to ensure that our information assets are adequately protected against unauthorised access or accidental disclosure. The existing ICT policy will be decommissioned. These policies will help us to deliver our vision, priorities and values.

3.2 The Information management policies are attached at Appendix A, and consist of:

- Data Protection Policy
- Information Security Policy
- Acceptable use of information and ICT Policy

4.0 Human resources/people management implications

4.1 The policies outline roles and responsibilities across the organisation in the implementation of the Information management policies.

5.0 Financial implications

5.1 There are no anticipated additional costs due to the policies alignment with the ICT review and strategy

6.0 Legal and data protection implications

6.1 The policies are intended to meet the council's legal and contractual obligations towards data protection, information rights and cyber security particularly PSN compliance and the forthcoming General Data Protection Regulation (GDPR)

7.0 Consultation

7.1 The draft policies were reviewed by the following: Legal, Policy, HR, ICT, Governance portfolio holder, trade unions

8.0 Risk management

8.1 The policies are designed to mitigate established threats to our information assets

9.0 Equalities Impact Assessment (EIA)

9.1 The main objective of the policies is to meet various legislation for data protection and information rights. The policies were reviewed for equalities and the following Equality Impact Assessments were conducted:

- Data Protection policy – Preliminary EIA (no negative impacts)
- Information Security Policy (covering information assurance/information classification and handling/physical security) - Preliminary EIA (no negative impacts)
- Acceptable use of information and ICT Policy – Full EIA (no negative impacts)

9.2 The Full Equality Impact Assessment is attached at Appendix B. No negative impacts have been identified.

10.0 Alternative options and reasons for rejection

10.1 Maintain existing policies. However the existing policies do not meet current information security objectives and will not meet the requirements of the General Data Protection Regulation that comes into effect on 25th May 2018

11.0 Recommendations

11.1 That Members consider the updated Information management policies.

11.2 That the proposed policies, attached at Appendix A, be approved and that the existing ICT Policy be decommissioned.

11.3 That changes to the policies be authorised after 25th May 2018 to reflect further guidance from the ICO, NCSC or other respected authorities, but that any changes will only be implemented after consultation with relevant senior leaders, senior managers and portfolio holder(s).

12.0 Reasons for recommendations

12.1 The policies provide a framework for the Council to continue to ensure that the information assets it holds are adequately protected thus allowing the council to deliver its vision, priorities and values.

Glossary of Terms *(delete table if not relevant)*	
GDPR	The General Data Protection Regulation (new European wide data protection law coming into effect on May 25th 2018.
ICO	Information Commissioner's Office (supervisory authority for data protection in the UK).
ICT	Information Communications Technology.
NCSC	National Cyber Security Centre (technical authority on Cyber Security in the UK).
PSN	Public Services Network.

Decision information

Key decision number	**Non-key 85**
Wards affected	**All**
Links to Council Plan	These policies will help the

priorities	council to deliver its priorities by contributing to ensuring that council services that rely on information assets and information systems are protected.

Document information

Report author	**Contact number/email**
Tony Smith	Tel: 01246 345 726 Email: tony.smith@chesterfield.gov.uk
Appendices to the report	
Appendix A	Information management policies: Data Protection Policy Information Security Policy Acceptable use of information and ICT Policy
Appendix B	Equality Impact Assessment for Acceptable use (of information and information systems) policy

This page is intentionally left blank

Data Protection Policy

Title	Data Protection Policy
Document version	1.0
Release date	1/5/2018
Author	Tony Smith
Consultation	• Cabinet member for governance • Corporate Management Team • Legal • Policy • Trade Unions • Arvato
Equality Impact Assessment	Please refer to the Information Assurance Equality Impact Assessment.
Review date	1 year from publication

Contents

Policy statement

It is council policy that all personnel will take responsibility for managing information in accordance with this Data Protection Policy.

This policy outlines how Chesterfield Borough Council (referred to as "the council" in this document) will protect its information assets by informing users of the data protection requirements that directly apply to them in their day to day handling of information to ensure its information is secure, allowing the information to be used effectively for delivering its services and data subject's rights are upheld.

Scope

All personnel, physical locations, information assets, supporting assets and 3rd parties as required.

Information assets in scope

All records created and held in all physical and electronic formats, including, but not restricted to:

- Paper
- Electronic / digital documents, including scanned images, databases and spreadsheets
- E-mail and voice mail
- Information held in blogs, wikis and discussion threads, and in other social media when used for business purposes, such as Twitter
- Visual images such as photographs
- Microform, including microfiches & microfilm
- Information stored on removable media, such as audio and video tapes, memory sticks, CDs, DVDs and cassettes
- Published web content (Intranet/Internet/Extranet)

Objectives

The main objectives of this policy are:

a) To uphold the rights of the data subject
b) To ensure everyone handles council information in accordance with the council's information assurance policies and guidelines
c) To manage risks to protect the confidentiality, integrity and availability of the information assets of the council affording additional protection to sensitive information
d) To comply with relevant legislation including the Data Protection act 2018 and the EU General Data Protection Regulation
e) To comply with contractual security requirements
f) To follow (where appropriate) information security best practices
g) To provide accountability to those people who protect the Council's information assets and supporting assets
h) To support efficient working practices

Roles & responsibilities

All personnel have a duty to ensure the council's information assets and information systems are used securely and efficiently.

Policies

1. Data Protection Principles

1.1. The council will ensure that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d) 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
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) 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

2. Lawfulness of processing personal data

2.1. The council will ensure that at least one of the following lawful conditions applies to each category of personal data processed for each purpose for processing:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose
b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations)
d) Vital interests: the processing is necessary to protect someone's life
e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

3. Processing criminal offences data

3.1. The council will only process personal data relating to criminal convictions and offences if a lawful basis for processing personal data (above) has been identified and processing is being performed either:

a) in an official capacity or
b) we have specific legal authorisation

3.2. The council will not hold a comprehensive register of criminal convictions unless we are doing so in an official capacity as established in law

4. Lawfulness of processing sensitive personal data

4.1. The council will ensure that the following special categories of personal data have a lawful basis for processing:

a) race
b) ethnic origin
c) politics
d) religion
e) trade union membership

f) genetics
g) biometrics (where used for ID purposes)
h) health
i) sex life or
j) sexual orientation

4.2. The council will ensure that at least one of the following lawful conditions applies to each category of sensitive personal data processed for each purpose for processing:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes…
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent…
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim…
e) processing relates to personal data which are manifestly made public by the data subject…
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity…
g) processing is necessary for reasons of substantial public interest…
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care…
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…

5. Data Subjects Rights

5.1. The council will maintain standard operating procedures to ensure the individual rights of data subjects are upheld namely:

a) The right to be informed
b) The right of access (subject access requests)
c) The right to rectification
d) The right to erasure (right to be forgotten)

e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling

5.2. Individual rights requests will aim to be resolved within one calendar month and free of charge

5.3. The council will maintain and provide privacy information to data subjects

6. Conditions for processing of personal data outside the United Kingdom or the European Union

6.1. The supervisory authority's guidance will be followed to ensure that any personal data processed outside of the United Kingdom or the European Union has an adequate level of protection and is in accordance with the law

7. Accountability and Governance

7.1. The council will maintain the designation of a Data Protection Officer

7.2. The council will maintain documentation for 'records of processing activities' of personal data

7.3. The council will maintain an 'Information Security Policy' to ensure appropriate technical controls are in place to protect personal data

7.4. The council will conduct data protection impact assessments where appropriate

7.5. The council will maintain suitable data protection training to staff and ensure it is part of their learning and development programme

7.6. The council will maintain its annual payment of the data protection fee to the supervisory authority (the Information Commissioner's Office) (ICO))

7.7. The council will also administer the annual payment of the data protection fee on behalf of councillors (with their consent)

7.8. The council will follow the supervisory authority's guidance to ensure that its processing of personal data is in line with the supervisory authority's best practices

7.9. The council will ensure contracts and data sharing agreements are in place to ensure all parties understand their responsibilities and liabilities for processing personal data

8. Personal data breaches

8.1. The council will report any relevant data breaches within 72 hours of becoming aware of the breach to the supervisory authority

8.2. The council will also inform data subjects without undue delay if a breach is likely to result in a high risk of adversely affecting the data subject's rights and freedoms

8.3. The council will maintain a log of any personal data breaches

9. Children's personal data

9.1. Particular attention will be afforded to processing children's personal data in accordance with the supervisory authority's guidance

This page is intentionally left blank

Information Security Policy

Title	Information Security Policy
Document version	1.0
Release date	1/5/2018
Author	Tony Smith
Consultation	• Cabinet member for governance • Corporate Management Team • Legal • Policy • Trade Unions • Arvato
Equality Impact Assessment	Please refer to the Information Assurance Equality Impact Assessment.
Review date	1 year from publication

Contents

Policy statement

It is council policy that all personnel will take responsibility for securing information in accordance with this Information Security Policy.

This policy outlines how Chesterfield Borough Council (referred to as "the council" in this document) will protect its information assets and supporting assets by the use of appropriate technical and administrative controls to ensure its information is secure, allowing the information to be used effectively for delivering its services.

Scope

All personnel, physical locations, information assets, supporting assets and third parties as required.

Information assets in scope

All records created and held in all physical and electronic formats, including, but not restricted to:

- Paper
- Electronic / digital documents, including scanned images, databases and spreadsheets
- E-mail and voice mail
- Information held in blogs, wikis and discussion threads, and in other social media when used for business purposes, such as Twitter
- Visual images such as photographs
- Microform, including microfiches & microfilm
- Information stored on removable media, such as audio and video tapes, memory sticks, CDs, DVDs and cassettes
- Published web content (Intranet/Internet/Extranet)

Objectives

The main objectives of this policy are:

a) To ensure everyone who handles council's information or supports the council's information systems understands their obligations as outlined in this policy
b) To manage risks to protect the confidentiality, integrity and availability of the information assets of the council affording additional protection to sensitive information
c) To comply with relevant legislation
d) To comply with contractual security requirements
e) To follow (where appropriate) information security best practices
f) To provide accountability to those people who protect the Council's information assets and supporting assets
g) To support efficient working practices

Roles & responsibilities

All personnel have a duty to ensure the council's information assets and information systems are used securely and efficiently.

Policies

1. Access Control

1.1. Access to information systems and information assets should be limited to only those individuals whose jobs require such access

1.2. Access control roles should be used and include the specific needs required for the job function

1.3. Privileged user accounts should be restricted to provide least privileges necessary to perform job responsibilities and should only be assigned to roles that specifically require privileged access

1.4. Users and administrators should be assigned a unique ID before allowing access to information systems and information assets and exception to this rule (i.e. shared accounts must be authorised)

1.5. The formal 'starters, leavers, changes' process should be used for user account authorisations

1.6. Security policies should be used to enforce technical controls such as account lockouts

1.7. Users processing card payments or administering card payment systems may require additional access control policies in accordance with PCI DSS

1.8. Users should ensure their passwords meet the council's password guidance

1.9. Default passwords should be changed at the earliest convenience

Further guidance on 'Access Control' can be found in the document 'Information Security Guidance' section 'Access Control').

2. Mobile Working

2.1. Devices used for home and mobile working should be registered with the ICT department

2.2. Devices used for home and mobile working should be pre-configured by ICT to provide adequate security controls including authentication and encryption where possible

2.3. Users should ensure that mobile devices are kept physically secure and are not left unattended in public spaces

2.4. Users accessing DWP and HRMC data remotely should be aware of the additional requirements of the DWP 'Memorandum of understanding'

Further guidance on 'Mobile Working (agile working)' can be found in the document 'Information Security Guidance' section 'Mobile Working).

3. Removable Media

To prevent unauthorised disclosure, modification, removal or destruction of information stored on media the following policies will apply.

3.1. Use of removable media will be limited and controlled by the ICT department

3.2. Removable media should be scanned for malicious software before it is introduced onto data networks to prevent the risk of malware spreading

3.3. Sensitive information held on removable media should be encrypted

3.4. Removable media no longer required, damaged or otherwise should be returned to the ICT department

Further guidance on 'Removable Media' can be found in the document 'Information Security Guidance' section 'Removable Media'.

4. Network Security

4.1. Changes to network equipment and network connection configuration should only be carried out by the ICT department

4.2. The ICT department are responsible for ensuring that the network is configured securely and is monitored

Further guidance on ‘Network Security’ can be found in the document ‘Information Security Guidance’ section ‘Network Security’.

5. Secure Configuration of devices

5.1. The ICT department are responsible for ensuring that applications, devices and other components are configured securely

5.2. Users are not authorised to make changes to applications, devices or other components that may affect the security

5.3. Users are not authorised to install software on council equipment

5.4. Users must contact the ICT department if software is required to be installed on council equipment

5.5. Users must not attempt to bypass, alter or disable software settings such as anti-virus software, VPNs or proxy settings

5.6. The ICT department are responsible for procuring, issuing and managing end user devices

Further guidance on ‘Secure Configuration of devices’ can be found in the document ‘Information Security Guidance’ section ‘Secure Configuration’.

6. Data at rest

Data at rest measures should be implemented to protect information and information systems.

6.1. Sensitive information should be encrypted on mobile devices

6.2. Consideration for encryption on servers or desktops should be given where sensitive information is stored

6.3. Consideration for pseudonymisation on servers or desktops should be given where bulk personal data or sensitive information is stored

Further guidance on ‘Data at rest’ can be found in the document ‘Information Security Guidance’ section ‘Data at rest’.

7. Data in transit

Data in transit measures should be implemented to protect information and information systems .

7.1. Appropriate protection should be used to protect data in transit including the use of:

- IPSEC VPNs
- TLS VPNs
- Secure email
- Egress secure file transfer

7.2. Supported ciphers and protocols should be used

7.3. Deprecated ciphers and protocols should not be used. These include the use of SSL and early versions of TLS (i.e. 1.0 or 1.1)

Further guidance on ‘Data in transit’ can be found in the document ‘Information Security Guidance’ section ‘Securing Data in Transit’.

8. Personally owned end user devices (Bring your own device or BYOD)

The use of personally owned devices is authorised as follows.

8.1. The user has accepted the council’s information security policy and guidelines for the use of personally owned devices

8.2. The user has registered their device with the ICT department

8.3. The ICT department have ensured that adequate licenses are available (i.e. Microsoft and Mobile Iron)

8.4. The user has provided the council assurances that their device is configured securely

8.5. The personally owned device will only be used to process the following categories of information:

- Personal Information Management (PIM)
  - Email
  - Calendar
  - Contacts
- Web based content including
  - Internet
  - Aspire intranet
  - Learning Pool Learning Management System
  - ResourceLink MyView (self-service only)
- Photos or videos taken by the devices camera

- Council social media updates such as Twitter and Facebook (authorised users only)

8.6. The personally owned device will NOT be used to process the following categories of information:

- large scale personal data
- cardholder data as defined by PCI DSS
- PSN originating data including DWP and HMRC data
- all OFFICIAL “SENSITIVE” information as defined by the HMG GSC
- other information determined as sensitive or critical to business functions
- General Data Protection Regulation “special categories” of personal data:
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade union membership
  - genetic data
  - biometric data
  - health data
  - person's sex life or sexual orientation
- General Data Protection Regulation personal data relating to criminal convictions and offences

8.7. The ICT department will initially configure the device but will not provide technical support of the personally owned device

8.8. The council including the ICT department will not monitor the personally owned device

8.9. The user will report any loss of their device to the ICT department

8.10. The ICT department will carry out appropriate revocation of access or removal of council data on the user’s personally owned device in the event that the device is reported lost or access has been revoked (including when the user leaves the organisation)

Further guidance on ‘BYOD’ can be found in the document ‘Information Security Guidance’ section ‘Personally owned end user devices (Bring your own device or BYOD)’.

9. Secure configuration of Web browsers

9.1. Web browsers must only be installed by the ICT department

9.2. The ICT department will only install common web browsers that ICT can configure to receive security updates for

9.3. Web browsers must not bypass proxy servers if proxy servers have been configured

Further guidance on ‘Secure configuration of web browsers’ can be found in the document ‘Information Security Guidance’ section ‘Web Browsers Security’.

10. Secure configuration of Cloud Services

10.1. Cloud services must be reviewed for information security risks prior to their procurement

10.2. Cloud services procured must include clarity as to whom is responsible for on-going information assurance arrangements

Further guidance on ‘Secure configuration of cloud services’ can be found in the document ‘Information Security Guidance’ section ‘Cloud Security Guidance’.

11. Secure Software Development

11.1. Software developed in-house or outsourced must meet software development best practices

11.2. Software developed in-house or outsourced must be tested prior to deployment

11.3. Software developed in-house or outsourced must be documented and under formal change control

11.4. Software developed in-house or outsourced must be tested for any security vulnerabilities prior to implementation

11.5. Software developed in-house or outsourced that is related to card payments must meet the PCI DSS requirements

Further guidance on ‘Secure Software Development’ can be found in the document ‘Information Security Guidance’ section ‘Secure Software Development’.

12. Protective Monitoring

<u>Log files</u>

12.1. Log files should be kept to aid monitoring and investigations

12.2. Log files should be retained for defined periods of time to meet various legal and contractual obligations

12.3. Log files should be held centrally where configuration allows to simplify log management

Protective monitoring

12.4. Detection of wireless access points to protect cardholder data should be implemented in accordance with PCI DSS

12.5. Detection of cardholder data or other sensitive information at rest on storage systems should be implemented

12.6. Intrusion detection and change detection techniques should be implemented at various points in the network to protect cardholder data and other sensitive information

12.7. Time should be synchronised and configured securely on critical systems

Incident Response

12.8. In the event of a significant security event an incident team must be constructed to triage the incident

12.9. Security incidents must be responded to within appropriate timeframes

12.10. Incident response for lost, stolen or misplaced end user devices must meet the PSN and NCSC guidance

12.11. Incidents must be reported to external parties in accordance with legal or contractual guidelines

Further guidance on ‘Logs’, ‘Protective Monitoring’ and ‘Incident Response’ can be found in the document ‘Information Security Guidance’ section ‘Protective Monitoring’.

Physical security

13. Secure areas

13.1. Physical security perimeters must be defined for each premise holding information assets or information systems

13.2. Security zones are to be used to separate areas of a premise that require different levels of protection as follows:

- Zone 0 is classed as a Public zone and affords the least level of security
- Zone 1 is classed as a Semi-public zone with increasing security controls in operation
- Zone 2 is classed as a Back-office zone with increasing security controls in operation
- Zone 3 is classed as a Restricted zone with increasing security controls in operation

13.3. Each security zone should have a perceived zoning boundary (implied or actual) and people must understand the rules, expectations and limitations associated with crossing it and operating within it

13.4. Security measures for a zone must not be excessive or inappropriate

13.5. Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access

Unattended equipment

14. Users must ensure that unattended equipment has appropriate protection as follows:

- terminating active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver
- logging-off from applications or network services when no longer needed
- securing computers or mobile devices from unauthorised use by a key lock or an equivalent control e.g. password access, when not in use
- collecting sensitive or classified information print-outs immediately from any printer that is not configured with a “locked print” function

Clear desk policy

15. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted as follows:

- Sensitive information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated
- Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

- Unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented
- Media containing sensitive or classified information should be removed from printers immediately
- “Locked print” function should be used on printers where available to hold sensitive or classified information until the user is present at the printer and enters their PIN

Protecting payment card devices from tampering or substitution

16. Payment card devices must be protected as follows:

16.1. Officers responsible for devices should maintain an inventory of authorised payment card devices. The device inventory should include:

- make
- model
- serial number
- photos of the device(s) in a good known state

16.2. The list of devices should be updated when devices are added, relocated, decommissioned, etc.

16.3. ICT should be given copies of the inventory of authorised payment card devices so they can hold a central inventory

16.4. Device surfaces must be periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device)

16.5. Officers must verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices

16.6. Officers must not install, replace, or return devices without verification that the request is genuine

16.7. Officers must be vigilant for suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices)

16.8. Officers must report suspicious behaviour and indications of device tampering or substitution to appropriate personnel (for example, to a manager, to the ICT Service Desk, or to the Information Assurance Manager)

Further guidance on ‘Physical Security’ can be found in the document ‘Information Security Guidance’ section ‘Physical Security’.

User education

17. Training

17.1. The council will provide appropriate training to users to help the council meet its information assurance objectives

17.2. Line managers are responsible for ensuring that relevant information assurance training is carried out for personnel under their management

18. Awareness Campaigns

18.1. A security awareness campaign will be operated to raise awareness for information assurance by the information assurance team (e.g. intranet articles, emails, meetings and presentations)

Further guidance on ‘User Education can be found in the document ‘Information Security Guidance’ section ‘User Education’.

Information Classification

19. Information shall be classified in accordance with the council's information classification guidelines (adopting the HMG Government Security Classifications) as follows:

19.1. All information is recognised as "OFFICIAL" by default and appropriate security measures should be adopted to protect the confidentiality, integrity and availability of the information

19.2. "OFFICIAL" information does not need to be labelled as such

19.3. The descriptor "SENSITIVE" may be used for the following categories of information:

- OFFICIAL-SENSITIVE PERSONAL To identify sensitive or very sensitive information relating to an individual or group, where inappropriate access could have damaging consequences
- OFFICIAL-SENSITIVE COMMERCIAL To distinguish commercial or market sensitive data, including that subject to statutory or regulatory obligations, that may be damaging to BIS or to a commercial partner if improperly accessed

19.4. "OFFICIAL-SENSITIVE" information may require additional handling instructions

Handling instructions

20. Handling instructions are encouraged to be used as follows:

20.1. Users must confirm the recipients are correct before transmitting sensitive information assets to prevent unauthorised disclosure of information. This includes:

- Identifying a caller before discussing sensitive information on the phone
- Establishing an email communication with non-sensitive information first before transmitting sensitive information to an email recipient to establish the recipient is the correct one

20.2. Users must ensure communication channels are secure before transmitting sensitive assets. This can be achieved by:

- Using a secure email system
- Using a secure file attachment or transfer system

20.3. Users should provide handling instructions as appropriate in documents or emails. For example:

- Handling instruction: Please do not distribute this document further without the approval of the sender
- Handling instruction: If you are not the intended recipient of this email please delete immediately and notify the sender
- Handling instruction: HAND DELIVERY ONLY. This document must not be sent by postal or courier services. Please ensure the contents of the document are not visible during delivery
- Handling instruction: This document must not be faxed
- Handling instruction: Not to be copied further without the author's approval
- Handling instruction: Not to be shared outside of recipient organisation
- Handling instruction: Not to be printed without the author's approval
- Confidential - for recipient only
- "To be opened by addressee only" – for use when sending staff personal information through the post

Further guidance on 'Information Classification' and 'Handling Instructions' can be found in the document 'Information Security Guidance' section 'Information Classification'.

Human resources information security

21. Information security requirements should be established in employment contracts. For example:
    - You will complete training as required to understand the organisation's data protection and information security policies and procedures
    - You will adhere to the organisation's data protection and information security policies and procedures
    - You will ensure that your routine conduct meets the organisation's data protection and information security policies and procedures
    - You are aware that failure to adhere to the organisation's data protection and information security policies and procedures may lead to the organisation's disciplinary process being invoked

22. Vetting of personnel (to help protect information) must be carried out in accordance with the vetting requirements of the job role and in accordance with the law including the following requirements:

    22.1. Vetting will utilise the HMG Baseline Personnel Security Standard (BPSS) or equivalent

    22.2. Vetting should be conducted once a candidate has been accepted but before they start employment

22.3. Where a candidate is due to start work but a vetting check has not been completed – managers will need to conduct a risk assessment in accordance with best practices and in accordance with various legislation

22.4. Line managers are responsible for ensuring that vetting check renewals are carried out in accordance with the vetting check renewals guidance

23. User registration (for access to ICT systems)

23.1. Line managers are responsible for ensuring that user registration activities are carried out including liaising with HR, ICT and other relevant departments (applies to new starters or users moving to other service areas)

23.2. Users accessing any information system whose information the council is responsible for (whether cloud based or on-premise) must still be registered with ICT (irrespective of whether they have yet been given an Active Directory user account and corporate email address)

24. On-going information security requirements (whilst a user is in post)

24.1. Line managers are responsible for ensuring that all personnel under their management are applying information security requirements in accordance with the organisation's policies and procedures

25. Termination of personnel

25.1. Line managers are responsible for ensuring that user de-registration activities are carried out including liaising with HR, ICT and other relevant departments and that any assets are collected from the employee and returned to the asset owner for re-provisioning

25.2. Information security responsibilities and duties that remain valid after termination or change of employment are communicated to personnel

26. Disciplinary process

26.1. Personnel are reminded that the council operate a formal and communicated disciplinary process and action against personnel who have committed an information security breach will be carried out in accordance with the council's disciplinary process and/or where applicable the service provider’s breach management policy

Further guidance on ‘Human Resources Information Security’ can be found in the document ‘Information Security Guidance’ section ‘Human Resources Information Security’.

Business continuity

27. Business Continuity

    27.1. Business Continuity will be managed in accordance with the Business Continuity policy

NOTE: Business continuity (and Emergency Planning) is currently coordinated by the Emergency Planning Officer through a partnership with Derbyshire County Council.

ICT disaster recovery

28. ICT Disaster recovery

    28.1. ICT are responsible for ensuring ICT disaster recovery plans are maintained

    28.2. ICT are responsible for ensuring ICT disaster recovery plans are tested (at least annually)

Governance (Information assurance)

29. The council will support the roles required to ensure the council's information assets and information systems are used securely and efficiently for example:

    - Senior Information Risk Owner
    - Data Protection Officer (see Data Protection policy)
    - Information assurance department
    - Information asset owners
    - Information asset administrators
    - Business process owners

30. Forums will be established to support information assurance objectives for example:

    - ICT/Cyber/Information security working group meetings (technical)
    - Information governance working group meetings (non-technical)
    - Risk management meetings

31. Information assurance in project management

    31.1. Information security must be included in the organisation's project management business processes to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project

    31.2. The project management methods in use must take into account:

a) information security objectives are included in project objectives

b) an information assurance risk assessment is conducted at an early stage of the project to identify necessary controls (usually prior to any procurement of solutions)

c) information assurance controls are reviewed (or specified) for any solution requirements (tenders and frameworks)

d) information assurance risk assessments are repeated at relevant project stages e.g.

- once a solution has been shortlisted (to provide a more relevant risk assessment against a specific product)
- on review of the business process (to capture risks within the specific business processes)

Further guidance on ‘Information assurance in project management’ can be found in the document ‘Information Security Guidance’ section ‘Information assurance in project management’.

32. To ensure protection of the organisation’s assets that are accessible by suppliers - Information assurance in suppliers and the supply chain will be maintained as follows:

32.1. Formal access must be obtained by either the Information Asset Owner, Information Assurance Manager or Senior Information Risk Owner before suppliers are given access to the council’s information systems and information assets

32.2. The risks must be understood and mitigated before suppliers are given access to the council’s information systems and information assets

32.3. Information security requirements for mitigating the risks associated with supplier’s access to the council’s information systems and information assets shall be agreed with the supplier and documented prior to access being granted

32.4. All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation’s information

32.5. ICT will maintain a detailed record of all suppliers accessing the council's information systems and information assets including attributes such as what information is accessed, how it is accessed, etc.

32.6. ICT are responsible for reviewing supplier's access requirements and disabling or removing access that is no longer required

33. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product in their supply chain

Acceptable use of information and ICT Policy

Title	Acceptable use of information and ICT Policy
Document version	1.0
Release date	1/5/2018
Author	Tony Smith
Location of published policy	aspire intranet
Consultation	• Cabinet member for governance • Corporate Management Team • Legal • Policy • Trade Unions • Arvato
Approved by	
Equality Impact Assessment	Please refer to the Information Assurance Equality Impact Assessment.
Review date	1 year from publication

Contents

1. Policy statement

It is council policy that all personnel will take responsibility for managing information in accordance with this Acceptable use of information and ICT Policy.

This policy outlines how Chesterfield Borough Council (referred to as "the council" in this document) will protect its information assets and supporting assets by highlighting to users the policies, guidelines, and key messages that directly apply to them in their day to day handling of information and use of information systems to ensure its information is secure, allowing the information to be used effectively for delivering its services.

2. Scope

All personnel, physical locations, information assets, supporting assets and third parties as required.

3. Objectives

The main objectives of this policy are:

1. To ensure everyone handles council information or uses the council's information systems in accordance with the council's information assurance policies and guidelines

2. To manage risks to protect the confidentiality, integrity and availability of the information assets of the council affording additional protection to sensitive information

3. To comply with relevant legislation

4. To comply with contractual security requirements

5. To follow (where appropriate) information security best practices

6. To provide accountability to those people who protect the Council's information assets and supporting assets

7. To support efficient working practices

4. Roles & responsibilities

All personnel have a duty to ensure the council's information assets and information systems are used securely and efficiently.

5. Instructions

5.1. Supporting policies & guidance

5.1.1. Users are reminded that information and information systems must be used in accordance with the following supporting policies and guidelines

- Data Protection policy
- Information Security policy
- Information Security guidance

5.2. Key messages are also provided below to form a simplified code of conduct for users

<u>Monitoring user's use of information systems</u>

In order to enforce its policies the council monitors the use of its information systems in accordance with the law.

<u>Disciplinary procedures for misuse of council information and information systems</u>

Personnel will be investigated in accordance with the council's disciplinary procedures. Any misuse by agency staff, contractors, or sub-contractors will be referred to their employers.

<u>Human rights</u>

The Human Rights Act 1998 gives certain rights to privacy for personal electronic communications in the workplace. The council reserves the right for authorised officers, in an act of investigating potential misuse or in supporting the council's systems, to access such communications.

Electronic documents may be inspected and copied as part of legal proceedings involving the council, under court procedures now known as 'disclosure'.

<u>Computer misuse</u>

The Computer Misuse Act 1990 covers unauthorised or malicious use of any computer system. It is used to prosecute hackers and people who write and distribute computer viruses deliberately.

It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access. This law protects against employees and members of the public who deliberately cause damage to systems or data. The Act also makes it illegal for a person to deliberately delete data or sabotage systems to the detriment of the council.

Harassment

It is possible to commit harassment by using e-mail to send a harassing message to someone or by downloading and distributing material from the internet that creates an intimidatory working environment. Harassment and discrimination are unlawful under the Equality Act 2010 and Protection from Harassment Act 1997.

As with any form of harassment under the anti-discrimination legislation, the intention of the parties is irrelevant. Every individual in the organisation has a duty to promote a non-intimidatory working environment.

Obscene Material

Publishing legally 'obscene' material is a criminal offence under the Obscene Publications Act 1959. This includes electronic storing and/or transmitting of obscene materials that would tend to deprave and corrupt or any paedophiliac material. Any instances of this nature found will be reported directly to the Police.

Defamation or false statements

Liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the internet will be responsible for it and liable for any damage it causes to the reputation of the victim.

In addition to the liability of the individual who made the libellous or false statement, the council may also be held liable. This could be either under the normal principles of:

- indirect liability because the council is considered responsible – known as 'vicarious liability'

or

- direct liability as a publisher because of providing the link to the internet or e-mail system

An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

Reporting ICT related faults to the ICT Service Desk

Employees reporting ICT related faults should contact the ICT Service Desk by phone ext. 5253 or by e-mail to the ICT Service Desk.

The fault report will be noted and logged onto the ICT Service Desk system. An ICT Support Officer, allocated to resolve the fault report, will contact you to discuss/remedy the fault as soon as possible.

Incident response for lost, stolen or misplaced end user devices

Users must report lost, stolen or misplaced end user devices to their line manager and to the ICT Service Desk.

Using removable media

The use of removable media is restricted.

Users must request the use of removable media via the ICT Service Desk.

Training

Users should ensure they have received suitable training before accessing information and information systems.

Hardware and Software Acquisition

Requests to purchase any hardware and software must be in accordance with the council's procurement and project management procedures. This includes all computer hardware, software or services. All ICT related purchases must be made via the ICT service.

Software licensing & copyright

Managers should ensure that appropriate licences are purchased for any software in use by their staff.

Copyright laws may apply differently for each piece of software. In general, the copyright to every piece of software run on a system is owned by whichever company or person wrote it. The council has a legal duty to make sure sufficient licenses of the correct type are present to cover the use of all software.

No software can be loaded onto council systems without the organisation holding the appropriate licence to operate the software. Licences held by individuals that are not

held in the councils name will not suffice. All software licences should be purchased via the ICT service.

Reporting information security incidents

It is the duty of all personnel to report incidents to their manager, to the ICT Service Desk and to the Information Assurance Manager .

Sustainability

The use of resources such as paper should be reduced as much as possible. The following measures should be followed where printing is required:

- Always use duplex capable printers (printing on both sides of the paper) wherever possible
- Do not print paper copies of e-mail trails (only print required extracts)
- Read documents on an electronic device without printing
- Distribute documents electronically (preferably as a link to a centrally held copy)

Ensure that all non-shared ICT devices (i.e. computers and printers) are switched off when not in use. Where access is practical ensure that devices are switched off at the wall socket to ensure that ICT devices do not continue to use any standby power.

All ICT equipment must be returned to the ICT service for disposal in line with the European WEEE disposal (Waste Electrical and Electronic Equipment) directive.

All consumable items (such as ink cartridges and laser printer toners) issued by ICT services must be recycled.

In order to reduce both costs and the waste of consumables, the council has an active programme to reduce the number of printers, with a move to centralised, shared print facilities.

Confidential waste

Staff should utilise the confidential waste facilities provided or request confidential waste facilities from their line manager where they have not been.

Use of the “internet”

- Use of the internet for personal use is permitted provided the following applies:
    - It is in the employees own time
    - It is on a reasonable and occasional basis
    - It does not cause any disruption, disturbance, inconvenience or degradation of the service
    - It does not interfere with the work of the council

    - It does not interfere with other employees doing their jobs (in situations where computer are shared with other users)
    - council e-mail addresses (ending in .gov.uk) are not used for any registration when using the internet for personal use

- The council reserves the right to not provide services over the internet that have an adverse effect on productivity or are abused by individuals or groups of employees

- Use of the internet can have severe legal implications both for the employee and the council. Misuse can lead to disciplinary, criminal and civil proceedings. Disciplinary action may include action for gross misconduct

- Use of the internet for making financial transactions on behalf of the council will only be permitted, using systems implemented or authorised by senior management

- Any use of the internet to make payments for personal reasons is made entirely at the risk of the employee and the council accepts no liability

- If you require legitimate business access to a site that is blocked by the internet content filtering system you can contact the ICT Service Desk. They will then review the website, but they will only unblock the website if it is safe to do so

- If you knowingly enter a site that may be construed as unfit, obscene or inappropriate this could be considered as gross misconduct and be subject to a disciplinary investigation

- You should report any website that may cause offence (and is not blocked) to the ICT Service Desk so that they can block future access

Use of the e-mail system

- Use of the e-mail system for personal use is permitted provided the following applies:
    - It is in the employees own time
    - It is on a reasonable and occasional basis
    - It does not cause any disruption, disturbance, inconvenience or degradation of the service
    - It does not interfere with the work of the council
    - It does not interfere with other employees doing their jobs (in situations where computer are shared with other users)
- Use of e-mail can have severe legal implications both for the employee and the council. Misuse can lead to disciplinary, criminal and civil proceedings. Disciplinary action may include action for gross misconduct.
- 'All User' e-mails to employees and to council members is strictly limited
- Authorisation for sending e-mail communications to large groups of e-mail recipients should be requested from the council's Communications & Marketing Department to ensure the appropriate communication channels are being used
- You must not read, delete, copy or modify the contents of anyone else's mailboxes, unless this has been authorised by the appropriate level of management
- If you receive e-mail that is inappropriate or abusive you must report it to your line manager and also to the ICT Service Desk (to see if they can block future occurrences)
- Do not open attachments from unsolicited e-mails and do not forward such items to any other recipients under any circumstances (please delete the e-mails)
- Do not open attachments or forward e-mails that include:
    - "jokes" or other "humorous" materials
    - "chain letter" type e-mails
    - unrecognised invoices
- It is the duty of every employee to ensure that the e-mail system is used correctly
- You should not subscribe to any mailing list that will send you material that conflicts with these guidelines
- You must not forward any sensitive information to your private e-mail address (either manually or via auto-forwarding)

- Any messages or information you send outside of the council, are statements that reflect on the council. Wherever appropriate, you must make it clear that the views expressed are personal and may not necessarily reflect those of the council
- Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the council. Always remember that any statement you make may still be construed as representing the council
- All information systems including the e-mail system are the property of the council. In certain circumstances your line manager or another appropriate authorised Officer of the council can be provided with access to your mailbox (for example if information in your mailbox is required to deliver a service)
- Requests for access to mailboxes should be directed to the ICT Service Desk with the approval of the appropriate line manager and it is the responsibility of the line manager to ensure that access to another user's mailbox is legal (advice from the Information Assurance Manager should be sought)
- Your line manager or an appropriate authorised Officer of the council can be provided with access your mailbox and/or any other data held in electronic format for the purpose of any disciplinary investigation. In this case confidentiality of your e-mail account and/or any other relevant data cannot be given. You are therefore advised that using the councils systems for any personal use (that you intend to be confidential) is unwise
- Use of personal e-mail storage (i.e. pst or ost files) for storing e-mails outside of the corporate e-mail system is not allowed
- All requests for increased mailbox capacity should be directed to the ICT Service Desk
- Users are reminded that increased mailbox capacity is only granted if the user has accepted their obligations to perform regular e-mail "housekeeping"
- Never use the e-mail system for knowingly doing anything illegal under UK law
- Never transmit sensitive information on e-mail unless you are certain that appropriate technical controls are in use
- Never abuse others - even in response to abuse directed at you
- Never use e-mail to harass or threaten other employees, Service users or anyone in any way

- Never use anonymous mailing services to conceal your identity or falsify e-mails to make them appear to originate from someone else
- Never access anyone else's mailbox unless they have given you proxy or authorisation rights or it has been agreed by senior management (unauthorised access is a breach of security and could be subject to disciplinary action)
- Don't use the 'Reply All' function unless everyone in the original message needs to know your response
- Don't print out messages routinely
- Don't create e-mail congestion by sending trivial messages or by copying e-mails to those who don't need to see them
- Don't send 'All User' e-mails. (ICT, Communications & Marketing and a few other users can send urgent communications if required)
- Respect any handling instructions included by the e-mail sender
- Remember e-mails may be read by a far wider audience than originally intended, because of the ease of forwarding messages to new recipients
- Remember e-mail is not guaranteed to arrive at its destination within a particular time, or even at all
- Remember not to send a message in capital letters. It is the electronic version of SHOUTING
- Remember any advice you give on e-mail has the same legal standing as any other written advice
- Remember before sending an e-mail, ask yourself how you would feel if your message was read out in Court or disclosed under Freedom of Information legislation
- Remember not to assume that the message has been read just because it has been sent
- Remember you can make reasonable and occasional personal use of the system, however this will be recorded and excessive use acted upon
- Remember to avoid sending graphics - it may look nice but it takes up valuable computer storage space and increases processing time
- Do maintain your Email mailbox properly
- Make sure that an `Out of Office' message is set up if you are away from the office for more than half a day

- Do only keep messages that are necessary for current business needs
- Do store all e-mail messages necessary for permanent business records in folders agreed with your line manager and according to current record retention policies
- Do delete insignificant, obsolete and unnecessary messages, return/read receipts and attachments, daily. Clear your `deletion' folder daily to get rid of unwanted items
- Do reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will or should be sent
- Do develop orderly filing systems for messages you need to retain
- Do always enter a subject title to your e-mail. Make sure that the 'subject' field of the message is meaningful. This helps everyone file and search for their messages more effectively
- Do try to use one message for one subject. Multiple subjects within a single message make it more difficult for the recipient to respond effectively, and to file the message
- Do think whether all your intended recipients really want or need to receive the message and any attachments

Email signatures

- Where available you must use a signature function to set an automatic signature to the bottom of your e-mails
    - For Microsoft Outlook this can be set at: File, Options, Mail, Signatures
    - For iPads and iPhones this can be set at: Settings, Mail, Signature
    - For Windows phones this can be set at: Mail app, settings, Signature=On

- Common requirements:
    - Arial 11 point
    - Text in black, non-bold and non-italic, not on a coloured or textured background/wallpaper and doesn't include a scanned or stylised signature image

New messages:

Your name (followed by limited post-nominals & qualifications in Arial 7 point)
Your job title
Your department or service
Chesterfield Borough council

Telephone: ##### ## ####
www.chesterfield.gov.uk

Approved graphic logos only (ask PR)

Replies / forwards:

Your name (followed by limited post-nominals & qualifications in Arial 7 point)
Your job title
Telephone: ##### ## ####

The council(s) websites

- No department within the council may establish a separate internet site unless this is formally authorised by senior management

- It is important that the information contained on the council's website is both accurate and up to date. It is the responsibility of officers to ensure website content for their service areas is accurate and up to date

- The council's Communications and Marketing service is the main point of contact for all enquiries regarding the News section of the council website

Where to store data

Data should be held centrally on the relevant server(s) and will be backed-up by the ICT Service in accordance with the requirements specified in the council's Business Continuity Plan. Data should not normally be held locally on a computer as it will not be backed up.

The Employee should contact the ICT Service if there is any doubt about whether data is being held on a computer and to discuss arrangements for backing up the data.

Taking photos

- Council supplied equipment that can take photos (such as Digital Cameras, Mobile Phones, etc.) must only be used for council business (in appropriate places at appropriate times). The use of such equipment for personal purposes or for any purpose that would bring the council into disrepute is strictly prohibited
- The use of personally owned ICT equipment that can take photos should be used in accordance with the personally owned devices (BYOD) guidance

Desk policy (data protection aspects only)

- You must not leave your computer unlocked (i.e. switched on and not password protected) when you are out of sight and not in direct control of the computer
- You must not leave documents containing sensitive information unattended
- You must lock away any documents containing sensitive information when not required
- Special attention must be given to protecting any information asset that is held in an area accessible by the public

Use of social media (data protection aspects only)

- You must not participate in any discussions that are inappropriate for the council to be involved with, whether locally or nationally, and you must not give advice or information that you know to be contrary to the council's policies or interests
- You must not reveal any confidential information online in a public forum
- Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private. Employees should never send abusive or defamatory messages

- Employees must also be security conscious and should take steps to protect themselves from identity theft (and phishing attacks), for example by restricting the amount of personal information that they give out

- Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:
    - ensure that no information is made available that could provide a person with unauthorised access to the council and/or any confidential information; and
    - do not publish or report on conversations that are confidential
    - do not publish or record any confidential information regarding the council on any social networking website
    - do not disclose personal data or information about the council, or its service users, employees or managers that could breach data protection law e.g. photographs, images
    - comply with data protection, intellectual property and copyright laws

Child Protection on Social media

- If an employee is moderating an online chatroom, online media or overseeing any content and activity where the participants will include children under 18 the employee will need to be DBS vetted to the level of an enhanced check (with a children's barred list check if activity is more than 3 times a month)

- Employees should not publish images of children or children and adults unless consent has been given in writing by someone with parental responsibility

Recruitment and social media

- At no stage during the selection process will searches on prospective employees be carried out on social networking websites

Intranets

- The council's "aspire" intranet is encouraged to be used by personnel for electronic discussions

Agile/Mobile working

- The screen on devices used for home and mobile working should not be visible and easily readable by others to protect sensitive information, for example on public transport, conference centres and meeting places

- Devices used for agile, home and mobile working carrying sensitive information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices

- You should seek prior authorisation to work outside your existing established council office building where the business process needs to meet specific security requirements or sensitive information is processed
- Users processing HMRC and DWP data have additional security requirements to meet. Do not assume that if you are given a device for agile working that you have met the requirements. Contact ICT Service Desk for advice

Note to ICT: Information Security requirements for Mobile/Agile working must be implemented in accordance with the council's Information Security Policy section "Mobile Working".

Password guidelines

We aim not to over burden users with passwords. However compliance frameworks such as PCI DSS stipulate strict password requirements.

If you are not processing cardholder data or other sensitive information and are experiencing issues with too many passwords please contact the ICT Service Desk who will check if the particular system can be reconfigured with less strict authentication requirements.

We will continue to adopt changes to passwords to reflect industry best practice.

How to select strong passwords or passphrases

- To create a strong password simply choose three random words. Numbers and symbols will also need to be included to meet the password complexity requirements.
- It is important to have strong and separate passwords for each account that you use, as a compromise of one system can lead to the other system being compromised with the same password.
- Never use any word which is related to you and may be easy to guess. Absolutely never use:
    - Current partner's name
    - Child's name
    - Other family members' name
    - Pet's name
    - Place of birth
    - Favourite holiday
    - Something related to your favourite sports team
- Never use passwords which are now considered 'weak'. They include:

- “password” and variants of it: Password/P@ssw0rd
- Months of the year even if it meets the complexity rules: December2017
- Seasons of the year even if it meets the complexity rules: Summer2017
- Common keyboard sequences such as: qwerty/12345/asdf
- Common numeric sequences such as: 12345/1111/01246/

How to remember strong passwords

- There are some simple memory tricks and techniques that could help you if you’re struggling to remember your strong passwords:
    - Loci method: imagine a familiar scene and place each item that needs to be remembered in a particular location i.e. red rose on the table, book on chair, poster on wall. Imagine yourself looking around the room in a specific sequence. Re-imagine the scene and the location of each item when you need to remember it
    - Story methods: remember a sequence of key words by creating a story and including memorable details e.g. ‘the little girl wore a bright yellow hat as she walked down the narrow street…’.
- Storing passwords. Passwords can be stored as follows:
    - Write your passwords down but store them in a safe place
    - Store them in a ‘password vault’ app or application such as:
        - LastPass
        - Dashlane
        - KeePass
        - 1Password

      Note: this is not an endorsement of any password manager.
    - Store them in your web browser (but only on a computer that you have logged into with your username and not on a public/internet café computer)
- Passwords must not be stored as plain text (unencrypted) within files on electronic folders

Re-using existing passwords or passphrases

- Do not re-use previously used passwords or passphrases that you know have been compromised (on any system at home or work)

NOTE: If you process payment card transactions then PCI DSS compliance does not currently allow you to re-use previously used passwords. You therefore may be a

member of a password policy that will prevent you from re-using existing passwords. This may also be true for password policies for other information deemed sensitive.

- Use separate passwords for home and work and understand the difference between ‘high value’ and ‘low value’ accounts and passwords

- High value accounts include:

    - Your corporate active directory / email account
    - online banking and online payment services
    - password manager 17ccounts
    - work accounts used to login to ICT systems
    - cloud storage
    - platform accounts (like Apple, Microsoft or Google)
    - federated ID (where you log into one account using the credentials from another, usually Facebook or Google)
    - any account that you would be devastated to lose (for example your favourite social media accounts)

- Low value accounts could include:

    - an account that has very little personal data
    - an account that can’t be used to spend your money
    - an account that doesn’t contain any personal information about other people
    - an account where there is no expensive or irreplaceable content (like photos, music, games etc)

- Crucially, if criminals steal one of these ‘low value’ passwords, it would only give them access to other low value accounts that share the same password. Your high value accounts, all of which should have unique passwords, would still be protected

Suspicion of compromised password or passphrase

- You must immediately change your password if there is any suspicion the password could have been compromised
- If you have used the same password on multiple systems (not recommended) then you will need to change the password on all of those systems that share the common password
- Report it if you believe your password could have been compromised

Sharing passwords

- Avoid sharing your password where it is not appropriate to do so

Using Wi-Fi

- Users accessing sensitive information must not connect to public Wi-Fi hotspots or conduct business in public areas including coffee shops
- Users must not disable the corporate VPN, anti-virus settings, disable proxy settings or any other setting that have been configured to protect the device

Note to ICT: Please refer to the Information Security Policy for guidance on securing Wi-Fi.

Procedures for handling council information

Users must familiarise themselves with the guidance for classifying information and the guidance for handling information.

Cloud based systems

Cloud based systems can be defined as the use of any information system that is not hosted on the council's premises and is hosted on the internet by a third party.

- User's must ensure that they have obtained permission to use a cloud based system before processing council information on it (this is to ensure that we meet our various contractual and legal obligations)
    - this is normally met by one or more of the following tasks:
        - Request to ICT
        - Discussing with the Information Assurance Manager and/or the service provider's security team as appropriate
        - Following the council's project management procedures

Note to ICT: Cloud based systems must be implemented in accordance with the council's "Cloud security guidance". Please refer to the Information Security Policy.

Use of encryption to protect information

- Encryption should be used where possible to help protect information from unauthorised access
- ICT will normally provide encryption facilities for sending e-mails securely or sending files securely. Contact the ICT Service Desk for assistance

Note to ICT: Encryption must be implemented in accordance with the council's Encryption Guidance". Please refer to the Information Security Policy.

End user devices

- council ICT equipment must not be used for any non-work related purposes (except as noted for permitted personal use) or in any way that will bring the council into disrepute

- All ICT equipment must be located, installed and operated in line with current policies regarding health and safety at work
- It is each employee's duty to ensure that all council ICT equipment is used responsibly in undertaking their duties for the council
- Any loss or damage to council ICT equipment (including any device or media with stored data) must immediately be reported to your line manager and to the ICT Service Desk
- All old / surplus or other ICT equipment that is no longer required by a service must be notified to the ICT Service Desk for reallocation or disposal
- You must not use the council's ICT systems for anything which is illegal or any of the following actions:
    - Promoting any commercial ventures, causes or organisations unless specifically authorised to do so by your line manager
    - Promoting any private or personal interests such as selling personal possessions / property, or promoting a social activity not related to the council
    - Publishing any material that, in whole or in part, appears to be designed to affect public support for a political party. This could take the form of political publicity, campaigning or lobbying
    - Sending, accessing, retrieving or storing any communications of a discriminatory or harassing nature, or materials that are offensive, obscene, pornographic, sexually explicit, incite hatred or depict violence
    - Using or transmitting abusive, defamatory, libellous, profane or offensive language
    - Representing values which are contrary to any council policies
    - Breaking through security controls, whether on the council's equipment or on any other computer system
    - Any activities that could knowingly cause congestion and disruption of networks and systems
    - Disclosure of any personal information in breach of data protection law
- The use of ICT systems for the procurement of goods and services is only permitted where these systems are part of an approved process, with agreed audit controls

Note to ICT: End user devices must be implemented in accordance with the council's "End User Devices Security Prerequisites Guidance". Please refer to the Information Security Policy.

Using personally owned devices (Bring your own device)

Users opting to use their own devices for accessing non-sensitive council information must familiarise themselves with the guidance for use of “Personally owned end user devices”.

Please refer to the Information Security Policy section “Personally owned end user devices (Bring your own device or BYOD)”.

Note to ICT: BYOD must be implemented in accordance with the council’s guidance for using personally owned equipment. Please refer to the Information Security Policy section “Personally owned end user devices (Bring your own device or BYOD)” for ICT requirements.

Chesterfield Borough Council

Equality Impact Assessment - Full Assessment Form

Service Area: Customers, Commissioning and Change
Section: Information Assurance
Lead Officer: Tony Smith

Title of the policy, project, service, function or strategy the preliminary EIA is being produced for: **Acceptable Use of IT**

Is the policy, project, service, function or strategy:

Existing ☐
Changed ☐
New/Proposed ✓

STEP 1 – MAKE SURE YOU HAVE CLEAR AIMS AND OBJECTIVES

What is the aim of the policy, project, service, function or strategy?

To help employees make the best use of the ICT systems and facilities, while protecting the Council's information assets to ensure information is secure and can be used effectively for delivering its services.

Who is the policy, project, service, function or strategy going to benefit and how?

The use of ICT can bring significant benefits to CBC activities and delivery of services. The policy helps employees to go about their work safely and within legislative requirements in relation to use of ICT systems and facilities.

What outcomes do you want to achieve?

- Remove the significant risks to CBC operations.
- To provide a safe framework for using ICT without exposing the council or employees to risk of its use.
- Ensure acceptable use of ICT
- Establish the parameters of appropriate use and best practice
- Protect the council and users form potential legal liabilities.
- Explain the consequences of breaching acceptable use.

What barriers exist for both the Council and the groups/people with protected characteristics to enable these outcomes to be achieved?

The reliance upon ICT systems and changing nature of information channels, for example social media.

STEP 2 – COLLECTING YOUR INFORMATION

What existing data sources do you have to assess the impact of the policy, project, service, function or strategy?

- Previous corporate ICT Policy (versions from 2010 and 2012)
- Policies from members of the East Midlands Councils WARP (including NEDDC).
- The National Cyber Security Centre, ISO 27001 & ISO 27002 official documentation and PSN compliance.

STEP 3 – FURTHER ENGAGEMENT ACTIVITIES

Please list any additional engagement activities undertaken to complete this EIA e.g. met with the Equalities Advisory Group, local BME groups, Employee representatives etc. Could you also please summarise the main findings.

Date	Engagement Activity	Main findings
12/12/2016	Review of policies by Governance portfolio lead	No equalities related comments.
21/2/2017	Review of policies by Business Transformation	Policies to be available in a range of formats to support accessibility.
31/3/2017	Review of policies by Gerard Rogers (Local Government and Regulatory Law Manager and	No comments on equalities.

	SIRO).	
24/5/2017	Review by unions.	Policies reviewed by GMB, UCAAT, Unite and Unison between 4th April and 24th May. No issues reported by GMB. Policies updated as a result of Unison's review. Nil response from UCAAT and Unite.
12/7/2017	Review by Arvato.	Policies reviewed by Arvato between 26th June and 7th July. No equalities issues raised.

STEP 4 – WHAT'S THE IMPACT?

Is there an impact (positive or negative) on some groups/people with protected characteristics in the community? (think about race, disability, age, gender, religion or belief, sexual orientation and other socially excluded communities or groups). You may also need to think about sub groups within each equalities group or protected characteristics e.g. older women, younger men, disabled women etc.

Please describe the potential impacts both positive and negative and any action we are able to take to reduce negative impacts or enhance the positive impacts.

Group or Protected Characteristic	**Positive impacts**	**Negative impacts**	**Action**
Overall impact - The policy takes into account legislative requirements, such as provisions within the Human Rights Act in relation to privacy. It also states that, at no stage during the selection process will searches on prospective employees be carried out on social networking websites.In line with the Equality Act, the policy protects employees and the public from harassment.			
Age – including older people and younger people.	The policy sets out guidance in relation to child protection and safeguarding when using social media.		
Disabled people – physical, mental and sensory			

including learning disabled people and people living with HIV/Aids and cancer.			
Gender – men, women and transgender.	See overall impact.		
Marital status including civil partnership.	See overall impact.		
Pregnant women and people on maternity/paternity.	See overall impact.		
Sexual Orientation	See overall impact.		
Ethnic Groups	See overall impact.		
Religions and Beliefs	See overall impact.		

From the information gathered above does the policy, project, service, function or strategy directly or indirectly discriminate against any particular group or protected characteristic?

Yes ☐
No X

If yes what action can be taken to stop the discrimination?

N/A

STEP 5 – RECOMMENDATIONS AND DECISION MAKING

How has the EIA helped to shape the policy, project, service, function or strategy or affected the recommendation or decision?

The policy promotes a positive impact by providing a safe system for all users. It tackles any potential negative areas e.g. cyber bullying or digital harassment.

Procedures are developed to ensure the distribution of this policy is adequate and accessible to all users

How are you going to monitor the policy, project, service, function or strategy, how often and who will be responsible?

Systems are monitored and authorised employees will be given access to this information.

Policy to be reviewed annually or following any Legislation changes.

STEP 6 – KNOWLEDGE MANAGEMENT AND PUBLICATION

Please note the draft EIA should be reviewed by the appropriate Head of Service/Service Manager and the Policy Service before WBR, Lead Member, Cabinet, Council reports are produced.

Reviewed by Head of Service/Service Manager
Name:
Date:

Reviewed by Policy Service
Name: Katy Marshall
Date: 05/17

Final version of the EIA sent to the Policy Service ✓

Decision information sent to the Policy Service ☐

This page is intentionally left blank