CABINET – 28TH MARCH 2018

SUBJECT: **DATA PROTECTION REFORM – UPDATES TO CORE POLICIES**

REPORT BY: **ACTING DIRECTOR CORPORATE SERVICES AND SECTION 151 OFFICER**

---

1. PURPOSE OF REPORT

1.1 To seek Cabinet approval for the adoption of the amended versions of four core information governance/security policies. The updates are required to meet the forthcoming requirements of the new General Data Protection Regulation, reflect industry best practice and underpin the Council's information security provisions.

2. SUMMARY

2.1 The General Data Protection Regulation (GDPR) will be directly applicable in the UK from 25 May 2018. A Data Protection Bill is currently progressing through Parliament that not only ensures the UK's compliance with the requirements of GDPR but also a new EU Law Enforcement Directive, aspects of the Digital Economy Act and national security considerations. As reported to Cabinet in October 2017, there will be a greater requirement for accountability and "Privacy by Design", greater rights for data subjects, including rights to know what the Council will do with their data and mandatory breach reporting within 72 hours. The maximum monetary penalty for breaching the Data Protection Act currently set at £500,000 will increase to the equivalent of €20 million or 4% of global annual turnover under GDPR.

2.2 GDPR comes at a challenging time when services must become leaner, requiring more efficient ways of working and collaborations with other organisations. Effective information governance controls to reduce risk to service users and to the Council are vital to this process. This presents an opportunity to make better use of all of the Council's information assets, not just those containing personal information, to aid service delivery and potentially save costs, as well as addressing increasing demands of requests made under FOI and associated information rights legislation.

2.3 This report summarises key updates to four information governance/information security policies to meet the forthcoming requirements of the new General Data Protection Regulation, reflect industry best practice and underpin the Council's approach to security, access and use of information.

3. LINKS TO STRATEGY

3.1 Information governance is a key part of the Council's corporate governance arrangements and is reflected in the Corporate Risk Register and Annual Governance Statement section of the Statement of Accounts.

3.2 Effective governance of the Council's information underpins all Council activities, safeguarding information assets and using them to maximum effect to help achieve the Council's Priorities and Wellbeing Objectives, as well as the seven Well-being Goals of the Future Generations Act (Wales) 2015:

- *A prosperous Wales*
- *A resilient Wales*
- *A healthier Wales*
- *A more equal Wales*
- *A Wales of cohesive communities*
- *A Wales of vibrant culture and thriving Welsh language*
- *A globally responsible Wales*

4. THE REPORT

4.1 The General Data Protection Regulation (GDPR) will be directly applicable in the UK from 25 May 2018 and a Data Protection Bill is currently going through Parliament to pull together protection of personal information with aspects of the Digital Economy Act and national security considerations. GDPR comes at a financially challenging time, when local authorities are looking for more efficient ways of working including more collaboration with other organisations. This requires effective information governance controls to reduce risk to service users and to the Council, but also presents an opportunity to make better use of all of the Council's information assets, not just those containing personal information.

4.2 One of the changes introduced by GDPR is an overarching principle of accountability for any activity involving personal information. Adoption of effective policies related to the management of information in all formats is a vital element of CCBC demonstrating its commitment in this area.

4.3 In October 2017 Cabinet approved updates to the Information Risk Management Policy, which modified the time period for updates by Heads of Service as Information Asset Owners to the Council's Senior Information Risk Owner (SIRO), together with embedding Privacy/Data Protection Impact Assessments at an early stage when using personal information in a new way.

4.4 A number of other core policies also require updates and are appendices to this report. The opportunity is being taken to refresh not only the policies that have a direct impact on processing of personal information but also on Access to Unpublished Information in line with the Council's legal duties. The changes to each policy are summarised below:

Changes to Data Protection Policy

4.5 The original policy was approved by Cabinet on 28 November 2000 in preparation for full implementation of the Data Protection Act 1998. The Council's commitment to protecting personal information has not changed but the policy has been updated to reflect the needs of the GDPR. In addition to the existing data protection principles being replaced, there is an increasing focus on the rights of individuals and definitions of personal information and special category data have also been updated. Responsibilities for evidencing accountability and for monitoring compliance have also been specified, together with key tools that the Council can use to evidence this.

Changes to Records Management Policy

4.6 The original policy was approved by Cabinet on 16 October 2013. The updated version includes the new GDPR statutory Data Protection Officer role; reinforces the role of each Head of Service as Information Asset Owners and their responsibilities in line with the Council's Information Risk Management Policy and reflects the evolution of the Information Governance Steward role from having a directorate remit to a more specific Service Area remit.

Changes to Access to Unpublished Information Policy

4.7 The original Code of Practice on Access to and Requests for Unpublished Information was approved by Council on 28 June 2005. 13 years of experience of handling requests for information under the Freedom of Information Act and associated legislation has demonstrated that a shorter, more focused policy is more useable, enabling the day to day processes for handling information requests to be adapted as necessary to ensure compliance with the law with minimal impact on daily service delivery and to account for changes in expectation from the Information Commissioner. The core principles of the original Code have been retained in a high level policy statement, with a greater emphasis on Open Data commitments. Detailed procedures for complying with the policy are detailed separately, with updates reviewed by Information Governance Project Team as necessary.

Changes to Information Security Policy

4.8 The current Information Security Policy has remained unchanged since May 2009. Whilst it was still fit for purpose, a number of minor revisions are required to reflect changes to job titles, updated IT Security standards, modified email policy and disclaimer and revised ways in which users now utilise IT through mobile technologies. To simplify the document some detailed password information has been deleted and the email and Internet usage policies have been segregated from the main document and added as appendices. The revised draft document has been reviewed by Human Resources, the Trade Unions and all Directorate Senior Management Teams and all comments made have been reflected in the revised draft.

5. WELL-BEING OF FUTURE GENERATIONS

5.1 This report contributes to the Well-being Goals as set out in Links to Strategy above. It is consistent with the five ways of working as defined within the sustainable development principle in the Act in that effective management of the Council's information will ensure reliable, high quality information is held which could be shared with other partners to ensure a joined up approach to providing services and preventing problems, as well as to enable close working with communities affected by the Council's activities. Reliable information also ensures that decisions are more robust now and in the long-term and preservation of the Council's historic record means that current and future generations can hold the Council to account for its decisions and learn from previous activities.

6. EQUALITIES IMPLICATIONS

6.1 There are no equalities implications of this report and its recommendations for groups or individuals who fall under the categories identified in Section 6 of the Council's Strategic Equality Plan. There is no requirement for an Equalities Impact Assessment Questionnaire to be completed for this report.

6.2 The Council provides FOI information in the format that the applicant requests and this combined with Welsh language responses to FOI requests made in Welsh contributes to compliance with the Council's Strategic Equality Objective 4 – Improving Communication Access and the Council's Welsh Language Standards Compliance Notice.

7. FINANCIAL IMPLICATIONS

7.1 Monetary penalties that can be levied for data breaches are increasing from £500,000 to the equivalent of €20 million or 4% of global annual turnover following the implementation of the General Data Protection Regulation (GDPR) in May 2018.

8. PERSONNEL IMPLICATIONS

8.1 There are no personnel implications related to this report.

9. CONSULTATIONS

9.1 All responses from consultations have been incorporated in the report.

10. RECOMMENDATIONS

10.1 It is recommended that Cabinet approves adoption of the amended versions of four core information governance/security policies as set out in Appendix 1,2 3, and 4 of this report.

11. REASONS FOR THE RECOMMENDATIONS

11.1 The updates are required to meet the forthcoming requirements of the new EU General Data Protection Regulation, reflect industry best practice and underpin our on-going campaign to assure information security within CCBC.

12. STATUTORY POWER

12.1 General Data Protection Regulation 2016; Data Protection Act 1998 (due to be repealed by the Data Protection Bill); Data Protection Law Enforcement Directive 2016 and UK Data Protection Bill (expected to be enacted during 2018).

12.2 Other privacy legislation such as Privacy and Electronic Communications Regulations 2003 and Human Rights Act 1998.

12.3 Information rights legislation such as Freedom of Information Act 2000, Environmental Information Regulations 2004, Re-Use of Public Sector Information Regulations 2015 and INSPIRE Regulations 2009.

12.4 Section 60 Local Government (Wales) Act 1994 on duty to maintain records, supplemented by the FOI Section 46 Statutory Code of Practice on Records Management.

Author: Joanne Jones, Corporate Information Governance Manager

Consultees: Paul Lewis, Acting Head of ICT and Customer Services and Council SIRO
Cllr Colin Gordon, Cabinet Member
Christina Harrhy, Interim Chief Executive
Dave Street, Social Services Director
Mark S Williams, Interim Corporate Director Communities
Bethan Manners, Principal Solicitor
Lisa Lane, Corporate Solicitor
Steve Jordan, IT Security Manager
Bev Griffiths, Information Officer
Carl Evans, Assistant Information Officer
Information Governance Project Team
Anwen Cullinane, Senior Policy Officer - Equalities & Welsh Language

Background Papers

- Cabinet report on allocation of Statutory Data Protection Officer role, 28th February 2018
- Cabinet report on preparation for Data Protection Reform, including an updated Information Risk Management Policy,18th October 2017

Appendices:
Appendix 1 – Data Protection Policy
Appendix 2 – Records Management Policy
Appendix 3 – Access to Unpublished Information Policy
Appendix 4 – Information Security Policy

APPENDIX 1

Caerphilly County Borough Council

Data Protection Policy

Version:	Version 4
Date:	February 2018
Author/s:	Corporate Information Governance Manager
Consultee/s:	Corporate Management Team; Senior Information Risk Owner; Legal Services; Information Governance Project Team
Approved by:	Cabinet
Review frequency:	Every 2 years
Next review date:	February 2020

Data Protection Policy

1. Policy objective

1.1 Administration and delivery of quality services involves processing personal information about people. The Council is committed to managing personal information effectively and legally to maintain confidence between those with whom we deal and the Council.

1.2 This policy describes Caerphilly County Borough Council's approach to personal information.

2. Scope and definitions

2.1 This policy covers the Council's obligations under all legislation applicable in the UK covering data protection and privacy, and references the definitions in the General Data Protection Regulation 2016 (GDPR).

2.2 'Personal Information' is defined as any information relating to an identifiable person who can be directly or indirectly identified. Certain categories of data are subject to additional protections, and includes:

- Criminal allegations, proceedings, outcomes and sentences
- Physical or mental health or condition
- Politics
- Racial or ethnic origin
- Religion or other beliefs of a similar nature
- Sex life
- Sexual orientation
- Trade union membership
- Genetics
- Biometrics (where used for identification purposes)

2.3 'Processing' personal information means any activity involving personal information throughout the information lifecycle, from collecting and creating the personal information, to using it, making it available to others when necessary, storing it, and disposing of it when no longer required.

2.4 The policy applies to all employees, elected members, and other individuals/organisations acting on behalf of the Council who have access to personal information that the Council is responsible for. Detailed procedures accompany this policy to direct the processing of personal information in a fair, lawful and transparent manner.

3. Data protection principles

3.1 Personal information of all stakeholders – current, former and prospective service users, employees, suppliers and others - will only be processed in compliance with laws on privacy and data protection, specifically adhering to the GDPR principles that personal information must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than necessary; and
6. processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2 The Council will demonstrate accountability in adhering to the rights of individuals set out in data protection law, including their right:

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- and rights in relation to automated decision making and profiling.

4. Accountability and monitoring

4.1 A Statutory Data Protection Officer (DPO) is designated to oversee the management of personal information Council-wide, reporting to the Council's Senior Information Risk Owner (SIRO).

4.2 Heads of Service as Information Asset Owners adhere to the Council's Information Risk Management Policy, supported by Service Area Information Governance Stewards.

4.3 Data Protection/Privacy Impact Assessments will be undertaken at an early stage whenever use of personal information is proposed and particularly during new collaborations.

4.4 A record of personal information processing activities is maintained by each Service Area, and the way that the information is managed is regularly evaluated using Privacy Impact Assessments where appropriate.

4.5 Clear and timely privacy notices are communicated that enable the subject of the data to understand how their personal information is being used.

4.6 Sharing of personal information is carried out in compliance with approved protocols, including the Wales Accord on Sharing Personal Information and data processor agreements.

4.7 Disposal of personal information will be strictly in line with the Council's Records Retention and Disposal Procedure.

4.8 Everyone processing personal information understands their responsibilities and receives appropriate information to support them, including annual training.

5. Complaints and data security incidents

5.1 Failure to comply with the law on data protection may result in:

- Serious consequences for individuals that the data relates to, including embarrassment, distress, financial loss
- Irreparable damage to the Council's reputation and loss of confidence in the Council's ability to manage information properly
- Monetary penalties and compensation claims
- Enforcement action from the Information Commissioner
- Personal accountability for certain criminal offences and for breaching the Employee or the Elected Member Code of Conduct

5.2 Complaints or concerns can be made to the Council's Data Protection Officer, and will be dealt with in accordance with the Council's Information Governance Complaints Procedure.

6. Related policies and resources

6.1 This policy should be read in conjunction with the following Council policies:

- Records Management Policy
- Information Risk Management Policy
- Access to Unpublished Information Policy
- IT Security Policy

6.2 Additional guidance and resources:

- For the public - see the Council's website.
- For employees - the Council's Information Governance intranet pages.

7. Further Information

7.1 Further Information is available from Data Protection Officer/Corporate Information Governance Unit, 01443 86 4322; dataprotection@caerphilly.gov.uk

APPENDIX 2

Caerphilly County Borough Council

Records Management Policy

Formatted: Font: 20 pt

Formatted: Centered

Version:	Version 1.~~5~~6
Date:	~~Oct 2013 (reviewed Nov 2015)~~February 2018
Author/s:	Corporate Information Governance ~~Unit (ICT Services – Corporate Services)~~Manager
Consultee/s:	Corporate Management Team; Senior Information Risk Owner; Legal Services; Information Governance Project Team
Approved by:	Cabinet

A greener place
Man gwyrddach

CAERPHILLY COUNTY BOROUGH COUNCIL CYNGOR BWRDEISTREF SIROL CAERFFILI

Review frequency:	Every 2 years
Next review date:	~~Oct 2017~~Feb 2020

A record is defined as: *'Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business'* ~~(BS ISO 15489, 2000).~~.

Formatted: Font: 20 pt, Bold, Not Italic

Commitment to records management

1. Caerphilly County Borough Council recognises that its records are ~~its~~ collective assets.

2. Records comprise the Council's corporate memory of its policies, services and decision-making processes and reflect its business requirements. The Council is dependent on its records to operate efficiently and to account for its actions.

3. The Council is committed to ensuring its records are maintained in accordance with the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act.

Objectives

4. The Council will effectively manage its records from planning and creation through to disposal to fulfil the following objectives:

   - Create and capture accurate, authentic, reliable and useable records to produce evidence and demonstrate accountability
   - Maintain records to meet the authority's business needs for as long as required for operational efficiency
   - Dispose of records that are no longer required in an appropriate manner
   - Protect vital records
   - Conform to legal and statutory requirements relating to record-keeping

Scope

5. This policy applies to all records created, received or maintained by current and former Council ~~staff~~employees, elected members, volunteers or those otherwise acting as ~~its~~ agents of the Council in the course of carrying out their Council business.

6. All types of records are covered, regardless of whether they are held electronically (including emails), on paper or audio-visual media, whether in English, Welsh or other formats or languages, and regardless of their age.

7. The policy covers records stored in any location, whether in office accommodation, corporate record centres, network drives, portable media (e.g. laptops and memory sticks) or held by other organisations on behalf of the Council, for example contractors.

8. The organisation's Record Retention and Disposal Policy should be consulted for detailed information on retention of records.

Responsibilities

All staff

9. All staff (permanent and temporary) are responsible for creating, managing, and timely disposal of accurate records to evidence the Council's activities.

~~Members~~
~~Members~~Elected members

10. Elected members create, use and manage Council information day-to-day, including outside the Council offices within their home or constituency office environment. Therefore it is crucial that ~~Members~~elected members understand their responsibilities to create and maintain this information appropriately.

Directors

11. Directors as members of the Corporate Management Team (CMT) must ensure the discipline of records management is given recognition and profile within the Council equal to management of other corporate assets such as staff and finance.

12. Directors are responsible for ensuring their directorates manage records effectively to provide evidence of the Council's activities, and that staff are supported accordingly. Individual Directorates must only develop records management policy and procedures in line with this corporate Records Management Policy.

Senior Information Risk Owner (SIRO)

13. The Council's SIRO is the Council's Information Governance Champion, and takes a leading role in ensuring CMT are briefed in order to make decisions on key records management issues that arise. ~~The SIRO is the Head of ICT Services and the Council's Data Protection Officer.~~ The SIRO chairs the Information Governance Project Team and takes the lead on developing

information governance policy and best practice, and cascading this information across the organisation.

Data Protection Officer

14. The Council's Data Protection Officer (DPO) is a specialist role introduced by the General Data Protection Regulation 2016 and reports to the highest level of the Council via the SIRO. The DPO oversees responsible management of all personal information processed by the Council, and makes sure that records containing personal information are suitably created, updated, shared, used, stored and disposed of at the end of the records lifecycle.

Heads of Service/Information Asset Owners

14.15. ~~Heads of Service~~Heads of Service are Information Asset Owners for their service area, and report to the SIRO regularly in line with the Council's Information Risk Management Policy. They have a crucial role in translating the Council's records management aspirations into reality by maintaining an awareness of how records are managed within their Service Area, being proactive in identifying potential improvements, and cascading corporate initiatives to their staff. Heads of Service are also responsible for monitoring records management practice within their Service Area to ensure best practice is adhered to~~, and providing reports as required~~.

15.16. Heads of Service must also ensure staff are fully supported in managing records effectively, and must ensure appropriate arrangements are in place for contractors and other partner organisations to adhere to the Council's high records management standards.

~~Directorate~~Service Area Information Governance Stewards

16.17. Information Governance (IG) Stewards sit on the Information Governance Project Team and have a key role in developing information governance best practice that fits the work of each ~~directorate.~~service. IG Stewards also ~~communicate~~support their Head of Service in communicating and ~~monitor~~monitoring compliance with records management best practice throughout their ~~directorates~~service.

Corporate Information Governance Unit and Records Centres

17.18. ~~The~~ Specialist staff within the Corporate Records Centres and Information Governance Unit ~~supports all divisions of the Council and Members~~support service areas and elected members by providing advice and guidance on all aspects of effective records management practices, including hard copy and electronic records.

~~Corporate Record Centres~~

18. ~~The Corporate Record Centres advise on storage and retention of hard copy records, working closely with Corporate Information Governance Unit to ensure consistency in records management practice across the Council and across all types of records (hard copy and electronic).~~

IT ~~Section~~Service

19. IT, including IT Security Team, advise on ~~certain~~technical aspects of creating ~~and~~, maintaining and disposing of electronic records in conjunction with Corporate Information Governance Unit.

Equalities and Welsh Language Team

20. This team~~, within Legal and Governance,~~ can provide guidance and support on language and format issues relating to Welsh, British Sign Language, Braille and other spoken languages where it relates to any records held by the Council.

21. Supporting documents

- Corporate Record Retention and Disposal Policy
- Information Risk Management Policy
- ~~Environment Directorate Retention Schedule~~
- ~~Social Services Directorate Retention Guidance~~
- Data Protection Policy
- IT Security Policy
- ~~Policy on Requests for and~~ Access to Unpublished Information Policy
- Publication Scheme
- Wales Accord on Sharing of Personal Information (WASPI)
- ~~Information Sharing Protocols (WASPI and non-WASPI)~~
- ~~Strategic Equality Plan~~
- ~~Welsh Language Scheme~~

Formatted: Font color: Black

APPENDIX 3

Caerphilly County Borough Council

Access to Unpublished Information Policy

Version:	Version 5
Date:	February 2018
Author/s:	Corporate Information Governance Manager
Consultee/s:	Senior Information Risk Owner; Head of Legal Services; Corporate Management Team, Information Governance Project Team
Approved by:	Cabinet
Review frequency:	Every 2 years
Next review date:	February 2020

A greener place
Man gwyrddach

CAERPHILLY COUNTY BOROUGH COUNCIL
CYNGOR BWRDEISTREF SIROL CAERFFILI

1. Guiding principles

1.1 Caerphilly County Borough Council values its information as a critical asset for effective service delivery. The Council aims to make as much information as possible available for consultation and re-use to facilitate open and transparent government, and for the benefit of the local and national economy.

1.2 The Council is committed to:

- openness and transparency in the way it conducts its business, encouraging partner organisations engaged in public service to do the same, to help improve public services and empower citizens;

- making as much information available as possible without copyright, patent or other control restrictions, subject to the terms of the Open Government Licence, to foster innovation in the local area and drive economic growth;

- respecting principles of privacy and confidentiality whilst making available information that is in the public interest, in line with laws governing the release of information;

- providing a prompt, courteous and comprehensive response to requests for information, presenting information in clear language, in a format that takes account of different needs and free of charge wherever reasonable;

- providing a right of complaint where an individual is not satisfied with the response received.

2. Scope of policy

2.1 This policy outlines the Council's commitment to making unpublished information available in accordance with principles of open government and with the law, which includes:

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Data protection law including the 1998 Act, the new 2018 Act, and the General Data Protection Regulations 2016
- Digital Economy Act 2017
- Protection of Freedoms Act 2012
- Re-use of Public Sector Information Regulations 2015
- INSPIRE Regulations 2009
- The Local Government (Access to Information) (Variation) (Wales) Order 2007
- The Access to Information Act 1985

2.2 This policy does not cover elected members' rights of access to information, as these rights are covered by a protocol in the Council's Constitution.

2.3 This policy does not cover the sharing of personal information with other organisations in order to deliver services to individuals. Provisions within data protection law together with agreements such as the Wales Accord on Sharing Personal Information (WASPI) would cover this activity.

3. Principal Information Access Laws

3.1 The principal laws that cover access to unpublished public sector information are described below. These laws and case law change from time to time, and the Council adapts to these changes to ensure full compliance with the law.

3.2 In cases where an applicant requests information which needs to be considered under more than one information access law, applicants will be advised of which information is being considered under which law and the relevant timescales.

Freedom of Information Act 2000 (FOI)

3.3 The FOI Act is a general right of access to unpublished information. Once in receipt of a request made in writing, the Council has a duty to confirm or deny whether information is held, and supply the information, normally within 20 working days, as long as an exemption does not apply.

3.4 The FOI Act also imposes a duty for the Council to proactively publish certain categories of information. To fulfil this duty, the Council has adopted the Information Commissioner's Model Publication Scheme for Local Government. The Publication Scheme can be found on the Council's website, but the information listed can be located in a variety of places as outlined in the Scheme, for example via the Council's website, library, or reception of main public buildings.

Environmental Information Regulations 2004 (EIR)

3.5 Information that is classed as 'environmental information' must be dealt with under EIR, rather than FOI. The definition of environmental information is very broad ranging, and can include information on the state of the environment e.g. flooding; on measures that affect the environment such as policies and legislation; and on state of human health and safety, the food chain, cultural/built structures, air pollution etc.

3.6 Requests can be made verbally as well as in writing; in some circumstances exceptions may apply where the public interest is against disclosure of information; and whilst the timescale is usually 20 working days, it can be extended in certain circumstances.

Data protection law (DPA)

3.7 A great deal of the information that the Council holds is personal data, and FOI does not make this information available to the public.

3.8 The Council takes its legal duty to protect personal information of individuals very seriously, and any request for information that contains personal data will be carefully

considered with reference to data protection law. This includes the 1998 Act (DPA), the General Data Protection Regulation 2016 (GDPR), the new UK Data Protection Act expected to be enacted during 2018, as well as the common law duty of confidentiality and the Human Rights Act 1998.

3.9 If any person wants access to information that is held about themselves they can make a Subject Access Request under data protection law.

Routine requests for information

3.10 Examples of a routine request could be a request for a copy of a document produced by a service area or a request for opening hours or details of service. The Council will not fully engage FOI, EIR or DPA procedures, but will seek to comply with the statutory deadlines.

4. Making a request for information

4.1 The Council would encourage any individual seeking to make a request for information from the Council to follow the guide on the Information Commissioner's website at www.ico.org.uk. In line with the Section 45 Code of Practice under FOI, the Council will provide applicants with advice and assistance in making requests for information.

4.2 In most cases requests for information must be made in writing (including email), but requests for environmental information can be made verbally. The request for information must include the following:

- a name and address to which a reply may be sent;
- sufficient detail for officers to identify what information is required - if a request does not contain enough detail, clarification will be sought from the applicant;
- in the case of a Subject Access Request, proof of identification is also required.

4.3 Applicants may express a preference for how the information is to be supplied and where reasonably practicable the Council will comply with the stated preference or provide an explanation if this is not possible.

5. Third party information that does not contain personal data

5.1 The approach to handling any request for third party information that is personal in nature is described in Section 3.3.

5.2 If non-personal information is requested from the Council that relates to a third party, for example a supplier or a partner organisation, the request will be considered with reference to exemptions available under FOI/EIR law, many of which are subject to a public interest test, to judge whether disclosure would be in the public interest.

5.3 The Council will endeavour to consult with third parties affected by disclosure of information as long as timescales permit, but the final decision must rest with the Council.

5.4 Contracts/agreements in place between the Council and partner organisations will include terms outlining the Council's legal responsibilities to consider disclosure of information on receipt of a request.

6. Charging for Information

6.1 The Council aims to make as much information as possible available free of charge. If there are charges for Council publications or information listed in the Publication Scheme, these charges will be advertised in advance.

6.2 The law enables a charge to be made to respond to a request for unpublished information in some circumstances, for example if it takes a significant amount of time to locate, retrieve or extract information to answer a request, or to cover the costs of communicating information to the applicant, e.g. for photocopying, printing and postage.

6.3 If a charge applies, it will be calculated in accordance with the law and guidance from the Information Commissioner, and will be explained to the applicant in advance.

6.4 There is no charge for inspection of public registers held at Council offices or for information held at public libraries including during normal working hours.

7. Equalities and Welsh language

7.1 The vast majority of information published by the Council is available bilingually, in line with Welsh Language Standards. If a request is made for unpublished information in Welsh, the information will be provided in the format in which it was originally produced, but the covering letter will be sent in Welsh.

7.2 The Council will make every effort to make information available in other formats. In some cases a charge will apply, and this would be explained to applicants in advance.

8. Complaints

8.1 The Section 45 FOI Code of Practice requires the Council to provide advice and assistance to people seeking information, to state the basis for any refusal of a request for information, and to provide advice on how to make a complaint.

8.2 Advice on how to make an Information Request Complaint can be obtained from Corporate Information Governance Unit on 01443 864322 or at foi@caerphilly.gov.uk.

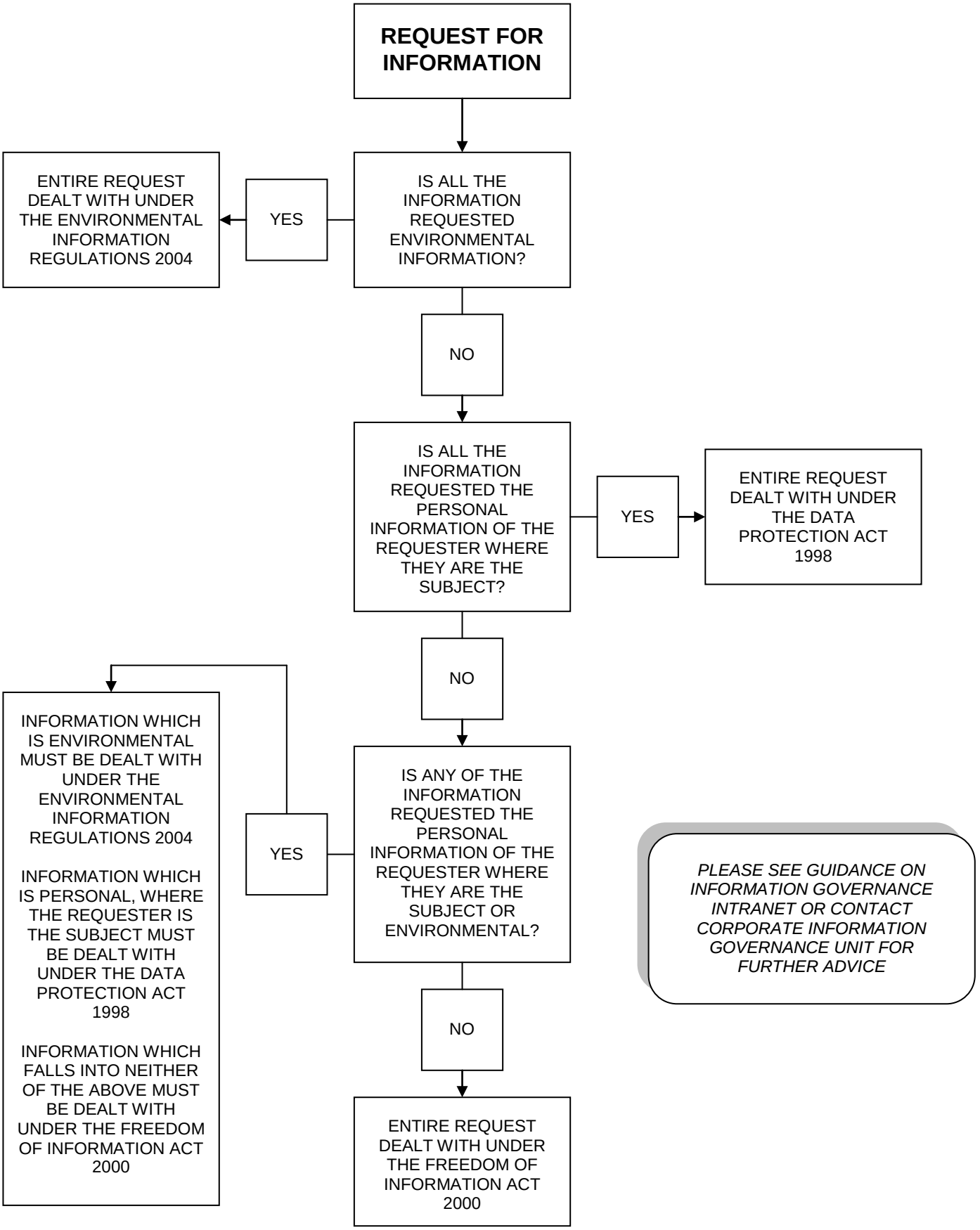
8.3 If the applicant is still not satisfied after the internal Information Request Complaint has been dealt with, they have a further statutory right of complaint to the Information Commissioner.

9. Related policies and resources

9.1 Caerphilly CBC Data Protection Policy

9.2 Caerphilly CBC Records Management Policy
9.3 Information Commissioner website www.ico.org.uk

Appendix 1 Which access regime is applicable?



Gwasanaethau Technoleg Gwybodaeth
Information Technology Services

ISO/IEC 27001 Information Security Management

CCBC Information Security Policy

A greener place to work
Man gwyrddach i gweithio

DOCUMENT CONTROL INFORMATION

Department: Information Technology Section

Title CCBC Information Security Policy

Reference PO-G-003

Date: Jan 2018

Version: 11.0

Author: Stephen Jordan/Wesley Colyer

Assurance: I.T. Security Forum

REVISION	DATE	REVISION DESCRIPTION
1.0	Jan 2006	Version for IT Security Forum
2.0	April 2006	Version for CITSG
3.0	May 2006	Live version after Council approval
4.0	Aug 2007	Amended following Internal Audit Review
5.0	Jan 2008	Amended to incorporate Mobile Policy reference
6.0	June 2008	Amended to incorporate updated Mobile Policy
7.0	Aug 2008	Amended to include IT Helpdesk changes
8.0	Oct 2008	Amended to include IT Training Start Date change
9.0	Feb 2009	Amended to include GCSX section
10.0	May 2009	Amended to include reference to Paper Documents (Information Unit)
11.0	Jan 2017	BS ISO27001:2013 version

REVISION	DISTRIBUTION LIST
1.0	IT Forum Members
2.0	IT Forum Group
3.0 – 11.0	All staff - Intranet
	DOCUMENT LIBRARY
ISMS – Secure Server	O:\IT\Shared\IT Security\ISO27001\Policies

Non-disclosure: The information contained in this document is confidential and is to be used solely by CCBC staff for I.T. Security references.
The contents of this document may not be disclosed in whole or part to any other third party organisation.

Table of Contents

1 INFORMATION SECURITY

1.1 Introduction

Caerphilly County Borough Council (CCBC) has, and will continue to make a large investment in the use of Information Technology, which will be used to the benefit of all directorates. Our information assets (encompassing facilities, data, software, paper documents and people) are essential for our day-to-day operational, financial and general information needs. It is therefore essential that the availability, integrity, and confidentiality of these corporate assets be protected against any potential security incident.

This Information Security Policy has been developed by IT Security and is based on the Code of Practice for Information Security Management under the International Standard BS ISO/IEC 27002:2013, and the Information Security Managements Systems - Requirements of the International Standard BS ISO/IEC 27001:2013.

The Information Security Policy is relevant to all information services provided, irrespective of the equipment or facility in use, and applies to:

a) All employees and agents;

b) Employees and agents of other organisations who directly or indirectly support or use the information technology services provided;

c) All use of information assets throughout Caerphilly County Borough Council.

d) Interested parties. (As defined by the ISO27001:2013 I T Security Standard)

Caerphilly County Borough Council takes information security very seriously, and any breach of this policy could lead to disciplinary action being taken against employees under the Council's agreed disciplinary procedure.

1.2 Definition

Information Security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities.

We must protect the confidentiality, integrity, and availability of Caerphilly County Borough Council's information assets.

To protect the confidentiality of our information assets we must ensure that our information is accessible to authorised users only.

To protect the integrity of our information assets we must safeguard the accuracy and completeness of our information and processing methods.

To protect the availability of our information assets we must ensure that our users have access to information and its associated assets in conjunction with agreed service levels.

1.3 Objectives and scope

There are three main objectives of this policy, which are detailed below: -

1. To ensure that the confidentiality, integrity, and availability of Caerphilly County Borough Council's information assets, are adequately protected from all threats, whether internal or external, deliberate or accidental;

2. To ensure that staff are aware of, and fully comply with, all *current and relevant security policies and legislation;*

3. Legislation. Caerphilly County Borough Council has to comply with all UK legislation affecting information management. All employees and agents must adhere in the provisions detailed in the Acts detailed below and future legislation that may be enacted: -

   a) The Data Protection Act, 1998 / General Data Protection Regulations 2018;
   b) The Computer Misuse Act, 1990;
   c) The Copyrights, Designs and Patents Act, 1988;
   d) The Regulation of Investigatory Powers Act, 2000;
   e) Electronic Communications Act, 2000;
   f) Freedom of Information Act, 2000.
   g) Human Rights Act 1998

4. To create and maintain, within all directorates, a level of awareness of the day to day importance of information security, and for all staff to understand their own information security responsibilities.

N.B. This policy must be read in conjunction with the E-Mail usage Policy and the Internet Usage Policy.

2 CORPORATE SECURITY POLICY STATEMENT

Objective

The objective of information security is to protect the confidentiality, integrity, and availability of the Councils information assets.

Policy

- The Chief Executive has approved the Corporate Security Policy Statement.
- The purpose of the Information Security Policy is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.
- It is the policy of the organisation to ensure that:
  - Information assets will be protected against unauthorized access;
  - Confidentiality of information assets will be assured;
  - Integrity of information will be maintained;
  - Regulatory and legislative requirements will be met;
  - Business continuity plans will be produced, maintained and tested;
  - Information security training will be available to all staff that use IT services;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Security Officers.
- Business requirements for the availability of information and information systems will be met.
- The Information Security Officers have direct responsibility for maintaining the Information Security Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Information Security Policy within their business area, and for adherence by their staff.
- It is the responsibility of all staff to adhere to the Information Security Policy.

3 SECURITY FRAMEWORK

Caerphilly County Borough Council adopts a proactive approach to information security management.

It uses the Code of Practice for Information Security Management under the International Standard BS ISO/IEC 27002:2013, and the Information Security Managements Systems - Requirements of the International Standard BS ISO/IEC 27001:2013 as the framework for setting control objectives and controls, including the structure of the Council's information assets risk assessment and risk management procedures.

4 CCBC MOBILE COMPUTING – POLICY

4.1 Definition of mobile devices covered by this policy

The definition of a mobile device for the purpose of this policy is any mobile computing device that is owned by Caerphilly County Borough Council that can be used to store or view information or data. These include, but are not limited to, the following: -

Laptop	External hard drives	
Notebook	External	CD
Tablet		CD-R
PDA		CD-RW
USB memory sticks (pen drives)		DVD
Card readers		DVD-R
Cameras		DVD-RW
USB memory cards	External disk drives	
	Smart Phone	

These devices can be standalone or have the ability to connect to a network.

4.2 Purpose

The aim of this policy is to ensure that all mobile computing devices issued to CCBC Staff and members have the required protection and security controls in place to ensure that the risk of information contained on the devices being compromised is minimised to an acceptable level. This includes physical protection (risk of theft), access controls, backup, virus protection, encryption, and connectivity to the Authority's network as well as defining what is acceptable and unacceptable use of such devices.

4.3 Use of Mobile Computing equipment

Mobile computing devices must only be used for Caerphilly CBC business. They must not be used for personal use. In particular it is strictly forbidden for a device to be connected to a private, or other phone line to facilitate personal Internet or E-mail use. Any access to the network using a mobile device will require the user to have a Username and Password as the minimum level of security authentication. This also applies to laptops, PDA's etc that do not connect to the network. Mobile devices may need to be connected to the Internet to gain communication back to the CCBC network, in these cases this must be done via a Virtual Private Network (VPN) arrangement that has been set up by CCBC IT Services.

When being used in public places, meeting rooms etc., steps should be taken to reduce the risk of information stored on a mobile device being overlooked by unauthorised persons.

4.4 Anti-Virus & Security updates

Mobile computing equipment must be updated regularly with the latest anti-virus software and security updates. For devices that are connected to the network this will be done automatically, however it is important that equipment is connected on a regular basis in order for the updates to take place. For stand-alone devices, virus software must be updated on a regular basis; advice on this can be sought from IT Security.

4.5 Encryption

Whenever possible information of a sensitive or confidential nature should not be stored on mobile computing devices. The appropriate corporate encryption solution must be used on all CCBC mobile devices. If in doubt consult IT Security**.**

4.6 Remote Access

Remote access across a public network (i.e. phone line) will only be allowed after authorisation has been obtained from an individual's Head of Service and approved by the Head of Information Communications Technology & Central Services or his appointed deputy. Authorisation for members of Council will be processed via Members Services, and confirmed by the Head of Information Communications Technology & Central Services or his appointed deputy prior to connection. Controls are in place to ensure that connection and user authentication to systems is from a legitimate source.

4.7 Non CCBC Mobile Computing Equipment / BYOD

Non-CCBC mobile computing devices must not be connected to any part of the CCBC network or any CCBC device, or used to store information belonging to the authority.

4.8 Physical Protection

Important: CCBC insurance only covers equipment on Council premises or employees homes. It does not cover equipment that has been left in vehicles, for example.

All mobile computing devices are valuable pieces of equipment and as such must be protected against theft and the risk of damage. Equipment should be kept with you at all times or stored in a secure location. If appropriate equipment can be further protected by the use of security products e.g. cable locks. Advice can be sought from IT Security in relation to this. Mobile equipment must not be left in a vehicle if at all possible. If it is necessary, steps should be taken to ensure that they are locked away securely out of sight, in a car boot for example, and for as short a time as possible. Equipment must not be left unattended in public places.

Any mobile computing device owned by Caerphilly County Borough Council must be returned when leaving the organisation or if it is no longer required.

4.9 Legislation

Where personal data about individuals is stored on mobile computing equipment this must comply with CCBC Data Protection guidelines. Advice on this can be obtained from our Corporate Information Governance Unit.

4.10 Auditing

The IT Security team reserve the right to recall mobile devices for auditing, to ensure compliance with this policy.

4.11 Corporate network connectivity

It is the responsibility of all laptop users (who have network access) to make their best efforts to ensure that the device is connected to the corporate network at least every 28 days (as a maximum). Connectivity to the corporate network is required in order to achieve compliance with CCBC encryption, anti virus, operating system updates, and auditing security protection we have in place.

4.12 Public Services Network (PSN - GCSx)

GCSx stands for Government Connect Secure Extranet, which is part of the GSI community.

It is a secure private Wide-Area Network (WAN), which enables secure interactions between connected Local Authorities and other government organisations, whose security management processes and procedures adhere to commercial best practice.

These are typically English and Welsh Local Authorities under the Department for Communities, and Local Government (DCLG) led Government Connect Programme.

4.13 Training and awareness

All new employees of Caerphilly County Borough Council will receive information security training and awareness via the Human Resources induction process undertaken by Managers.

There is a continuous security awareness programme in place for existing employees, issued periodically by I.T. Security officers.

4.14 Business continuity

System backups of computer hosts, and servers operating on the corporate network will be taken on behalf of users by IT Services and other authorised personnel at agreed predefined frequencies.

System backups for all other stand-alone computer systems located within directorates are the responsibility of the staff within the relevant directorate.

The safekeeping and availability of physical records located within directorates is the responsibility of the staff within the relevant directorate.

5 SECURITY RESPONSIBILITIES AND SECURITY INCIDENTS

5.1 Security responsibilities

Information security is the responsibility of Caerphilly County Borough Council as a corporate entity and all members of staff, and agents.

The Information Security Policy will apply to all staff and agents that use information assets, whether they are computer hosts, servers, network, PC, mobile users, paper records, and electronic data.

Senior and line managers in service areas are responsible for the policing of the Information Security Policy. Any queries or questions regarding the policy, please contact the IT Helpdesk or IT Security.

5.2 Security Incidents

It is the duty of all members of staff to report any suspected breach of information security to their Head of Service and the IT Security Officers.

Examples of information security events and incidents are:

a) Loss of service, equipment or facilities;

b) System malfunctions or overloads;

c) Human errors;

d) Non-compliance with policies, guidelines, rules

e) Breaches of physical security arrangements;

f) Uncontrolled system changes

g) Malfunctions of software or hardware;

h) Access violations.

6 SECURITY RULES

6.1. Computer Equipment

The IT Services Department is responsible for the control and maintenance of all computer equipment within the authority.

No equipment may be connected to the network or attached to any equipment connected to the network without prior authorisation of I.T. Security.

The 'Policy for Mobile Equipment' ensures the proper use of mobile equipment, owned by Caerphilly County Borough Council.

The aim of this policy is to ensure that all mobile computing devices issued to Caerphilly County Borough staff, have the required protection and security controls in place to ensure that the risk of information contained on the devices being compromised, is minimised to an acceptable level. The policy states that 'Non-CCBC mobile computing devices must not be connected to any part of the CCBC network or device, or used to store information belonging to the authority.

It is forbidden to install, disconnect or move any computer equipment.

This is the responsibility of the IT Services, Installation and Support Team.

It is forbidden to remove any Caerphilly County Borough Council information asset stickers.

Desktop, servers, and portable computers (laptops, tablets, Smart Phones etc.) must not have any software installed, removed or modified without authorisation from the IT Services Department.

Computer equipment must not be used for any personal or private work.

Computers must not be left unattended, logoff your computer when you leave your desk, power off your computer when you finish work.

6.2 Network Access

Access to the Council's private corporate data network is restricted to authorised employees and agents and is conditional that you comply with the CCBC Information Security Policy.

Staff requests to provide access to the network must be made to the IT Services Helpdesk using the User Profile Request Form.

A staff request for remote access to the network is granted when IT Security, has receipt of a signed and authorised Request for Remote Access form. This request has to be approved by the Head of Information Communications Technology & Central Services or his appointed deputy.

Staff (agents) from outside organisations or companies must not be given access to any computer systems without the permission and involvement of IT Security.

Third party access to the corporate network is only granted by IT Security on receipt of a signed and approved Third Party Access Contract, which is obtained from IT Security.

6.3 Data Storage Drives - Usage

Information stored on any storage drives must not breach Data Protection Legislation, and confidential information must not be made available for any unauthorised access.

The following must not be stored on any network drives:

- Information that is not related to the business of Caerphilly County Borough Council.
- Pornographic, offensive, derogatory or discriminatory material.
- Unauthorised or illegal software.
- Non-business images or executable files/programs.
- Games or non-business applications.

6.4 Passwords

Passwords must not be disclosed to anyone, written down or displayed in a way, which would allow the password to become known to unauthorised staff or members of the public.

The use of another persons Login ID and password is strictly forbidden. Login information setup by the IT Services department is specific to the user the login was created for and

must not be shared with other users. Employees will be held liable for any misuse of a computer resulting from the use of their Login ID and password.

6.5 Information

Information held on Caerphilly County Borough Council's information technology computers or subsequent output, for example, printed letters/tabulations, is the property of Caerphilly County Borough Council and is governed by the provisions of Data Protection Legislation.

Data Protection Legislation requires that computer processing of data relating to living individuals, i.e. personal data, be registered with the Crown appointed Registrar. Information required for registration includes details of the type of data, the purpose for which the data is held, and the sources and disclosure of data. There are a number of offences, which, if the provisions of the Act are not complied with, will affect the Council, and its employees.

The general provisions of Data Protection Legislation are:-

- all processing of personal computer data must be registered;
- personal data must only be processed as specified in the registration;
- computer personal data must not be disclosed to an unauthorised person;
- on request, and when appropriate for a fee; individuals have a right to a written copy of the data held; requests should be directed to the Corporate Governance Information Unit;
- appropriate security measures must be taken to protect computer personal data.

Any queries relating to the provisions of Data Protection Legislation should be directed through your line manager, to the Corporate Information Governance Unit.

6.6 Virus Protection

All Caerphilly County Borough Council computers are protected by virus detection software. This software must be operational at all times and never deactivated by the users. Any detected viruses must be reported to IT Services immediately.

All software (whatever media) must be virus checked before it is copied to any Caerphilly County Borough Council device.

6.7 Software Copyright

The copying of proprietary software programs or the associated copyrighted documentation is prohibited and is an offence which could lead to personal criminal liability with the risk of a fine or imprisonment.

The loading of proprietary software programs for which a licence is required but not held is prohibited.

Personal software should not be loaded onto Caerphilly County Borough Council devices under any circumstances. If the software is deemed to be of use to the organisation then it should be duly acquired under licence via IT Services.

6.8 Computer Misuse

All employees should be aware of their access rights for any given hardware, software or data, and should not experiment or attempt to access hardware, software or data for which they have no approval or need to access to conduct their duties.

The following is regarded as misuse of Caerphilly County Borough Council's information assets.

Fraudulent activity such as: -

- altering input in an unauthorised way;
- destroying, suppressing, misappropriating computer output;
- altering computerised data;
- altering or misusing programs.

Distributing a program with the intention of corrupting a computer process.

Theft of data, software or hardware, including copyright infringements.

Using illicit copies of software, which may also infringe copyright law.

Unauthorised use of Caerphilly County Borough Council's computer facilities for private gain or benefit.

Unauthorised disclosure of information from computer input or output to unauthorised personnel.

Deliberately gaining unauthorised access to a computer system, usually through the use of communications facilities.

Interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.

Introduction of pornographic or other unsuitable offensive material, on to the corporate network.

6.9 System Monitoring

To protect the Council, employees, service users and public funds, the Council will monitor the use of IT activity in order to ensure the proper and lawful use of the system and will be performed by I.T. Security Officers or I.T. Management. Requests for I.T. Security Officers to monitor users I.T. activity must be in writing and have at least Head of Service authority containing the reasons for the request. Such monitoring will be undertaken in line with the Data Protection Code, Part 3 Monitoring at Work.

Requests for I.T. Security Officers to monitor users I.T. activity must be in writing and have at least Head of Service authority containing the reasons for the request, including a Privacy Impact Assessment. Requests will be checked with Exemption Panel'.

6.10 Acquisition and Disposal of Information Technology Equipment

All acquisitions must be in accordance with the provisions of the organisation's information technology strategy and its financial regulations and standing orders.

All acquisitions of additional hardware and software must be made via or with the approval of the Head of Information Communications Technology & Central Services or appointed deputy. All purchases of additional information technology equipment must be made via IT Orders and accompanied by a Business Case justification.

The disposal or permanent handing over of equipment, media or output containing personal or sensitive data must be arranged via IT Services to ensure confidentiality.

Prior to the disposal of any PCs, IT Services should be consulted to arrange for the permanent removal of all data and programs unless the recipient is taking over the software licence or is authorised to use it.

Disposals must be in accordance with the provisions of financial and environmental regulations and standing orders, which require the approval of the Head of Information Communications Technology & Central Services and the Head of Procurement & Customer Services.

IT Services will conduct all corporate equipment disposals.

6.11 Paper Files and Records

All employees must ensure that:

- Paper records are kept secure; for active records these should be kept in lockable filing cabinets making sure they are only accessible to authorised personnel on a 'need to know' basis. Inactive/semi active records should be kept in a secure storage area.

- Sensitive personal information must not be left on desks and must be locked away when not required.

- Records are kept for at least the minimum length of time (for retention periods refer to your departmental Retention Schedule, or contact the Records Management team for advice).

- Records can be accessed when required.

- Records scheduled for destruction are disposed of in an appropriate manner to ensure confidentiality is maintained.

7 PUBLIC SERVICES NETWORK (PSN)

PSN stands for Public Services Network (previously called GCSX Network - Government Connect Secure Extranet), which is part of the GSI community.

It is a secure private Wide-Area Network (WAN), which enables secure interactions between connected Local Authorities and other

organisations, whose security management process and procedures adhere to commercial best practice.

These are typically English and Welsh Local Authorities under the Department for Communities, and Local Government (DCLG) led Government Connect Programme.

All Local Authorities in England and Wales have been instructed by Central Government to use this secure network.

8 POLICY VIOLATIONS

Violations of security procedures established within this Information Security Policy must be reported to the Head of Information Communications Technology & Central Services or IT Security. Violations may include, but are not limited to, any act that: -

a) Exposes Caerphilly County Borough Council to actual or potential monetary loss through the compromise of information technology security;

b) Involves the disclosure of confidential information or the unauthorised use of personal and/or corporate data;

c) Involves the use of data for illicit purposes, which may include violation of the law, regulation, or any reporting requirement of any law enforcement or government body.

9 SOCIAL MEDIA ACCESS

Not all staff are granted Social Media access. For those that have access to Social Media staff are reminded that the council has a Social Media Policy and that even for staff using Social Media channels when not in work that there is advice and guidance within the Social Media Policy that is useful to them.

10 POLICY COMPLIANCE

I have read, understood and acknowledge receipt of the CCBC Information Security Policy. I will comply with the guidelines set out in this policy (including the Email, Internet, and Mobile policies) and understand that failure to do so might result in disciplinary or legal action.
N.B. E-mail usage and Internet usage are separate policies and must also be read and agreed to when accepting this policy.

Signature: _____ **Start Date**:_____

Printed Name:_____

Job Title:_____

Directorate:_____

Department:
_____

Team:_____

Site/Location:_____

Telephone Number:_____

The above fields **must** be completed before a Network/Email account can be created.

Please tick for access required:

Network User ID ☐ _____

Email ☐ _____

On completion please forward this page to:

I.T. Service Desk, Penallta House, Tredomen Park, Ystrad Mynach, Hengoed, CF82 7PG

APPENDIX 1

Classification – Official

Gwasanaethau Technoleg Gwybodaeth
Information Technology Services

CCBC E-Mail Usage Policy

Document Filename	CCBC Information Security Policy
Author:	Stephen Jordan / Wesley Colyer
Date:	Jan 2018
Document Status:	Version 11.0

DOCUMENT CONTROL INFORMATION

Department: Information Technology Section

Title CCBC E-Mail Usage Policy

Reference PO-G-006

Date: January 2017

Version: 1.1

Author: Stephen Jordan / Wesley Colyer

Assurance: I.T. Security Forum

REVISION	DATE	REVISION DESCRIPTION
1.0	Nov 2015	Version for I.T. Security Forum
1.1	Jan 2017	Amended following Trades Union consultation

REVISION	DISTRIBUTION LIST
1.0 – 1.1	I.T. Forum Members
	DOCUMENT LIBRARY
ISMS – Secure Server	O:\IT\Shared\IT Security\ISO27001\Policies

Non-disclosure: The information contained in this document is confidential and is to be used solely by CCBC staff for I.T. Security references.
The contents of this document may not be disclosed in whole or part to any other third party organisation.

E-MAIL USAGE POLICY.

The purpose of this policy is to ensure the proper use of Caerphilly County Borough Council's email system and make users aware of what CCBC deems as acceptable and unacceptable use of its email system. Should policy amendments be required, then staff will be made aware and Trades Unions consulted prior to any amendments being implemented. For any Legislative amendments required both staff and Trades Unions will be notified in a timely manner. This policy is applicable to all Caerphilly County Borough Council employees and agents.

LEGAL RISKS

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If you knowingly send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and CCBC can be held liable.
- If you knowingly forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and CCBC can be held liable.
- If you unlawfully forward confidential information, you and CCBC can be held liable.
- If you unlawfully forward or copy messages without permission, you and CCBC can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and CCBC can be held liable.

In order to minimise the legal risks to both yourself and to the Council, it is prohibited to:

- Knowingly send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and CCBC can be held liable.
- Knowingly forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and CCBC can be held liable.
- Unlawfully forward confidential information, you and CCBC can be held liable.
- Unlawfully forward or copy messages without permission, you and CCBC can be held liable for copyright infringement.
- Send an attachment that contains a virus, you and CCBC can be held liable.
- Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks.
- If you receive an email of this nature, you must promptly notify your supervisor.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Send email messages using another person's email account.

It is not necessary to obtain permission of an outside sender to forward that person's email, however please have regard for passing on indiscriminately something that was copyright.

Additionally there are a number of Acts that can be applied to E-Mail use:

- Data Protection Legislation (The Data Protection Act, 1998 & the General Data Protection Regulations, 2018)
- The Computer Misuse Act, 1990
- The Copyrights, Designs and Patents Act, 1988
- The Regulation of Investigatory Powers Act, 2000
- Electronic Communications Act, 2000
- Freedom of Information Act, 2000
- Monitoring at Work - Code of Practice, 2003
- The Human Rights Act 1998

GOOD PRACTICES

CCBC considers email as an important means of communication and recognises the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an email as they would for any other communication. Therefore CCBC wishes users to adhere where possible to the following guidelines:

- Writing emails:
  - Write well-structured emails and use short, descriptive subjects.
  - CCBC's email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smileys however, is prohibited.
  - External email signatures must include your name, job title and company name.
  - A disclaimer will be added underneath your signature (see Disclaimer)
  - Users should spell check all emails prior to transmission.
  - Do not send unnecessary attachments.
  - Do not write emails in capitals.
  - If you require any action by the recipient ensure they are included in the ''To' field not the CC or BCC fields.
  - If you forward emails, state clearly what action you expect the recipient to take.
  - Only send emails of which the content is appropriate. If they cannot be displayed publicly in their current state, consider rephrasing the email, or use other means of communication.
  - Only mark emails as important if they really are important.
  - Please ensure that Senior Officers are only included into e-mails that require their attention.
  - Please note that by copying Senior Officers into e-mail communications does not ensure they agree with your e-mail or are authorizing your actions.
- Replying to emails:
  - Where possible internal emails should be answered within 3 working days, please try to answer priority emails within 1 working day.
  - Replying to External emails should fall in line with the authority's policies on responding to letters.
- Out of Office notifications:-
- It is good practice to activate your Out of Office messages (Internal and External) when not in the workplace. N.B. These need to be in Welsh followed by English and can follow the two recommended

wordings detailed at the end of this policy.

- Users of GCSX E-Mails need to activate Out of Office messages within the GCSX E-Mail browser separately in addition to their Outlook e-mail messages.
- Newsgroups:
  - Users need to request permission from their supervisor before subscribing to a newsletter or news group.
- Maintenance:
  - Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

PERSONAL USE

It is strictly forbidden to use CCBC's email system for anything other than legitimate business purposes. For example, the sending of personal emails, chain letters, junk mail, jokes and executables is prohibited. All messages distributed via the Council's email system are CCBC's property.

The Council and the Trade Unions have agreed that the email system may be used for communication between an individual and his or her trade union, or vice versa, for matters relating to the individual's employment with the Authority. This will not be classed as personal use.

However, should an individual be concerned over access to their works email accounts, they should consider receiving Union emails to their personal email accounts or request that any communications are sent via a password protected attachment to the email.

CONFIDENTIAL INFORMATION

Please be aware of the security implications when sending confidential information via the email system. Confidential information needing to be emailed to other public sector organisations should be via GCSX email and to other third parties should be by encrypted e-mail using Egress Switch.

ENCRYPTION

Users may not encrypt any emails without obtaining written permission from their supervisor. If approved, the encryption key(s) must be made known to the council. The Council's preferred encrypted email solution is Egress Switch.

EMAIL RETENTION

Staff are responsible for ensuring that emails that constitute Council records or are of significance in other ways are moved to suitable repositories. Such facilities may be provided by line of business application software, electronic document management systems or suitably secured network drive locations. Once this has been done successfully, emails should be deleted from Outlook. All information must be managed in compliance with Data Protection Legislation and the Council's retention timescales.

.

SYSTEM MONITORING

To protect the Council, employees, service users and public funds, the Council will monitor the use of the email system in order to ensure the proper and lawful use of the system and will be performed by I.T. Security Officers or I.T. Management. Requests for I.T. Security Officers to monitor users I.T. activity must be in writing and have at least Head of Service authority containing the reasons for the request. Such monitoring will be undertaken in line with the Data

Protection Code, Part 3 Monitoring at Work. Such monitoring will be primarily confined to address/heading unless there is a valid and defined reason to examine content such as potential offences under the Computer Misuse Act, compliance with the Information Security policies and the Officers Code of Conduct.

If there is evidence of a failure to follow the guidelines set out in this policy, CCBC reserves the right to take disciplinary action.

INFORMATION REQUESTS

The Council has a statutory duty to comply with information requests made under Data Protection Legislation, Freedom of Information Act 2000, and associated legislation. All users of the Council's IT systems must be aware that this will require searching any information held by the Council, including on email systems, networked drives and mobile devices, and considering disclosure in line with the law.

DISCLAIMER

The following disclaimer will be added to each outgoing email:
Anfonir yr e-bost hwn at ddibenion darparu gwasanaethau'r Cyngor. Mae'r e-bost a'r atodiadau yn gyfrinachol ac fe'u bwriedir yn unig at ddefnydd yr unigolyn neu'r endid y cyfeirir atynt. Os ydych wedi derbyn yr e-bost hwn mewn camgymeriad, rhowch wybod i DiogeluData@caerffili.gov.uk drwy anfon e-bost yn ôl a dinistriwch yr holl gopïau heb eu hanfon at unrhyw drydydd parti. Sylwch fod unrhyw safbwyntiau neu farn a gyflwynir yn yr e-bost hwn yn perthyn i'r awdur yn unig, ac nid ydynt o reidrwydd yn cynrychioli rhai'r Cyngor. Yn olaf, dylai'r derbynnydd wirio'r e-bost hwn ac unrhyw atodiadau ar gyfer presenoldeb firysau. Nid yw'r Cyngor yn derbyn unrhyw atebolrwydd am unrhyw ddifrod a achosir gan unrhyw firws a drosglwyddir drwy'r e-bost hwn.

Os hoffech i ni gyfathrebu â chi mewn ffordd benodol, rhowch wybod i ni. Rydym yn croesawu gohebiaeth yn Gymraeg, yn Saesneg neu'n ddwyieithog (yn ôl eich dewis) neu mewn ieithoedd a fformatau eraill. Byddwn yn ymateb yn eich dewis iaith, ac ni fydd gohebu â ni yn Gymraeg yn arwain at unrhyw oedi.

I ddarganfod mwy am sut mae'r Cyngor yn gweithredu, ewch i'n gwefan yn: www.caerffili.gov.uk ac am ragor o wybodaeth am bethau i'w hystyried wrth gyfathrebu â ni drwy e-bost, ewch i http://www.caerffili.gov.uk/ebost

---

This email is sent for the purpose of delivering Council services. The email and attachments are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify DataProtection@caerphilly.gov.uk by return email and destroy all copies without passing to any third parties. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Council. Finally, the recipient should check this email and any attachments for the presence of viruses. The Council accepts no liability for any damage caused by any virus transmitted by this email.
If you'd like us to communicate with you in a particular way please let us know. We welcome correspondence in Welsh, English or bilingually (according to your

choice) or in other languages and formats. We will respond in your declared chosen language and corresponding with us in Welsh will not lead to any delay. To find out more about how the Council operates please visit our website at: www.caerphilly.gov.uk and for more information about things to consider when communicating with us by email, visit www.caerphilly.gov.uk/email

Should the employer require access to emails issued or received from a trades union or its member further dialogue is to take place with the Head of HR and Head of IT Services prior to any access being granted.

Questions
If you have any questions or comments about this Email Policy, please contact the IT Service Desk tel. 01443-864111 or IT Security tel. 01443-863227.

If you do not have any questions CCBC presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

OUT OF OFFICE SAMPLE WORDING for non monitored emails.
Dydw i ddim ar gael tan (DD/MM/YYYY) ac ni chaiff eich e-bost ei ddarllen yn fy absenoldeb. Byddaf yn ymdrin â'ch e-bost ar ôl dychwelyd i'r gwaith. Os bydd eich ymholiad yn un brys cysylltwch …
I am currently unavailable until (DD/MM/YYYY) with no access to my emails. My emails are not being monitored in my absence. Your email will be responded to following my return to work. If your communication is urgent please contact…

OUT OF OFFICE SAMPLE WORDING for monitored emails.
Dydw i ddim ar gael tan (DD/MM/YYYY), fodd bynnag bydd eich e-bost yn cael ei flaenyrru at (Insert another officer's email address and external telephone number) yn fy absenoldeb.
I am currently unavailable until (DD/MM/YYYY), however your email will be forwarded to (Insert another officer's email address and external telephone number) in my absence.

APPENDIX 2

Classification – Official

Gwasanaethau Technoleg Gwybodaeth
Information Technology Services

CCBC Internet Usage Policy

Document Filename	CCBC Information Security Policy
Author:	Stephen Jordan / Wesley Colyer
Date:	Jan 2018
Document Status:	Version 11.0

DOCUMENT CONTROL INFORMATION

Department: Information Technology Section

Title CCBC Internet Usage Policy

Reference PO-G-007

Date: January 2017

Version: 1.1

Author: Stephen Jordan / Wesley Colyer

Assurance: I.T. Security Forum

REVISION	DATE	REVISION DESCRIPTION
1.0	Nov 2015	Version for IT Security Forum
1.1	Jan 2017	Amendments following Trades Union comments

REVISION	DISTRIBUTION LIST
1.0 -1.1	IT Forum Members
	DOCUMENT LIBRARY
ISMS – Secure Server	O:\IT\Shared\IT Security\ISO27001\Policies

Non-disclosure: The information contained in this document is confidential and is to be used solely by CCBC staff for I.T. Security references.
The contents of this document may not be disclosed in whole or part to any other third party organisation.

Caerphilly County Borough Council - Internet Usage Policy.

The purpose of this policy is to ensure the proper use of Caerphilly County Borough Council's Internet facilities and make users aware of what Caerphilly County Borough Council deems as acceptable and unacceptable use of the Internet. Should policy amendments be required, then staff will be made aware and Trades Unions consulted prior to any amendments being implemented. For any Legislative amendments required both staff and Trades Unions will be notified in a timely manner. This policy is applicable to all Caerphilly County Borough Council employees and agents.

LEGAL RISKS

Internet facilities enable the user to access a very wide range of information, including personal data, linking to large numbers of computers and other individuals across the world. In this relatively uncontrolled environment, it is particularly important that users are aware of and conform to legal requirements:

- If you view, create, access, download or publish material that is pornographic, libelous, defamatory, offensive, racist or obscene, you and Caerphilly County Borough Council can be held liable.
- If you unlawfully view, create, access, download or publish confidential or personal information, you and Caerphilly County Borough Council can be held liable.
- If you unlawfully or without permission view, create, access, download or publish material that is copyrighted, you and Caerphilly County Borough Council can be held liable for copyright infringement.

Additionally there are a number of Acts that can be applied to Internet use:

- Data Protection Legislation (The Data Protection Act, 1998 & the General Data Protection Regulations, 2018)
- The Computer Misuse Act, 1990
- The Copyrights, Designs and Patents Act, 1988
- The Regulation of Investigatory Powers Act, 2000
- Electronic Communications Act, 2000
- Freedom of Information Act, 2000
- Monitoring at Work - Code of Practice, 2003
- The Human Rights Act 1998

ACCESS TO THE INTERNET

Access to Internet facilities will be authorised only via established procedures that require the user to agree to conform to this policy.

ACCEPTABLE USE

The primary purpose for a user to have access to Internet facilities is to enhance the efficiency and effectiveness of that user's work for the Council.

Caerphilly County Borough Council's Internet facilities must only be used for legitimate business purposes, personal use is prohibited.

The Council and the Trade Unions have agreed that the Internet system may be used for communication between an individual and his or her trade union, or vice versa, for matters relating to the individual's employment with the Authority. This will not be classed as personal use.

UNACCEPTABLE USE

Caerphilly County Borough Council's Internet facilities must not be used to view, create, access, download or publish material that is:

- Pornographic or Adult
- Racist, offensive, or derogatory
- Obscene
- Bullying
- Violent
- Fraudulent
- Likely to cause harassment to others
- Confidential
- Prejudicial to the Council's best interests
- Not relevant to the business of the Council
- Likely to irritate or waste time of others
- Likely to breach copyright

It is unacceptable to use Caerphilly County Borough Council's Internet facilities for:

- Gambling
- Shopping (including online auctions, holidays, cars etc.)
- Gaming
- Instant Messaging (IM) (e.g. Microsoft Messenger)
- Utilising Peer to Peer (P2P) applications (e.g. Napster or Kazaa)
- Accessing personal web mail (e.g. Hotmail, Yahoo, Wanadoo)
- Publishing or creating personal websites or pages
- Accessing chat rooms
- Accessing newsgroups other than those on an approved list

It is prohibited to use Caerphilly County Borough Council's Internet facilities for downloading:

- Software *
- Music, videos, etc.
- Games

* If required, business related software may be downloaded provided it is from a legitimate and secure source and that a member of staff from IT Services carries out the download. The software must be virus checked before installation.

Any accidental access to inappropriate content must be reported to IT Security.

SECURITY

To address the security risks posed by having access to the Internet the Council has a number of security controls (Anti-Virus applications, Firewalls and Web-filtering software) in place to protect its network and information systems.

It is prohibited to:

- Circumvent, or attempt to circumvent these or any other security controls that are in place.
- Gain or attempt to gain unauthorised access to information (e.g. by introducing keyloggers, spyware or malware).
- Attempt to test or detect weaknesses in the security infrastructure (e.g. testing firewalls, cracking passwords).
- Attempt or intentionally disrupt the normal functioning of the Internet or related services (e.g. by downloading illegal software or introducing viruses).

SYSTEM MONITORING

To protect the Council, employees, service users and public funds, the Council will monitor the use of the email system in order to ensure the proper and lawful use of the system and will be performed by I.T. Security Officers or I.T. Management. Requests for I.T. Security Officers to monitor users I.T. activity must be in writing and have at least Head of Service authority containing the reasons for the request. Such monitoring will be undertaken in line with the Data Protection Code, Part 3 Monitoring at Work.

If there is evidence of a failure to follow the guidelines set out in this policy, Caerphilly County Borough Council reserves the right to take disciplinary action.

The Council uses web-filtering software to control access to websites and pages and to monitor user activity. The software will block access to websites, pages or content that is inappropriate or not relevant to the business of the Council.

SOCIAL MEDIA ACCESS.

Not all staff are granted Social Media access. For those that have access to Social Media staff are reminded that the council has a Social Media Policy and that even for staff using Social Media channels when not in work that there is advice and guidance within the Social Media Policy that is useful to them.