REPORT TO CORPORATE RESOURCES OVERVIEW & SCRUTINY COMMITTEE

PORTFOLIO AREA: Learning & Development

Corporate Resources O & S
Date of Meeting: THURSDAY 16 October 2008

Public

Key Decision: No **Recorded in Forward Plan: No**

Inside Policy Framework

Title: **ICT Security Policy - Annexes**
Report of: **Director of Corporate Services**
Report reference: **CORP56/08 – ICT Security Policy - Annexes**

Summary:
This report presents the Annexes to the ICT Security Policy.

Recommendations:

1) The Corporate Resources Overview and Scrutiny Committee are asked to comment and put forward any amendments they wish to be considered for incorporation into the Annexes.

Contact Officer: John Nutley **Ext:** x7250

1. BACKGROUND INFORMATION AND OPTIONS

1. Corporate Resources Overview & Security (CROS) considered the ICT Security Policy on 4th September 2008.

2. That report outlined the overarching principles that would underpin the policy. The policy also made reference to annexes that would provide much of the detail on how the policy would operate.

3. The management of the appendices are designed in such a way that they may be modified and redrafted as circumstances change within ICT and the Council, with the ownership of them being delegated to the Information Systems Group.

4. CROS expressed a wish to have a sight of the annexes when they were complied and also to receive a presentation on their content.

5. The appendices are attached to the paper and the officer attending the meeting has prepared a presentation.

6. CROS are asked for their views, comments and suggestions on the annexes.

CONSULTATION

2.1 Consultation to Date.

2.2 Consultation proposed.
There is to be an extensive consultation exercise carried out with staff, Members and partner organisations to raise awareness of the annexes and the responsibilities they carry with them.

RECOMMENDATIONS

The Corporate Resources Overview and Scrutiny Committee are asked to comment and put forward any amendments they wish to be considered for incorporation into the Annexes.

IMPLICATIONS

- Staffing/Resources –
  An exercise in briefing staff will need to be carried out
- Financial –
  None
- Legal –
  None
- Risk Management –
  The adoption of the Policy and Annexes will reduce the threat to the Council's information systems.
- Equality Issues –
  None
- Environmental –
  None
- Crime and Disorder –
  None

ICT Security Policy Annexes

Version 2.0 06/10/08

Index

Securing Hardware, Peripherals and Other Equipment 3

Controlling e-Commerce Information Security 8

Processing Information and Documents 10

Purchasing and Maintaining Commercial Software 18

Developing and Maintaining In House Software 21

Combating Cyber Crime 24

Complying with Legal & Policy Requirements 27

Planning for business continuity 30

Addressing Personnel Issues Relating to Security 32

Controlling e-Commerce Information Security 35

Premises Security 37

Detecting and Responding to IS Incidents 39

Description	Securing Hardware, Peripherals and Other Equipment
Author	John Nutley
Version	1.0
Approval Date	Draft

Overview:
The Council recognises the investment it has made and continues to make in computer equipment and the contribution this can make to the efficiency and effectiveness of our staff.

It is important to ensure the resources of the Council are used appropriately. That prior to the purchase of any equipment a suitable business case has been approved and the correct procedures are followed during procurement.

It is also important it is recognised that the Council's equipment and resources are subject to the provisions of this annex through their whole life cycle up to and including disposal.

Purpose:
The aim of this annex is to state the principles that will govern the purchase use and disposal of computer hardware, computer peripherals and other associated equipment. These principles are designed in such a way that will enable this equipment to be used to their fullest extent but in a manner which is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers or other agents who have access to our computers or computer networks.

Policy Principles:

Purchasing and Installing Hardware

1. All purchases of new systems, hardware or new components for existing systems must be made in accordance with the Council's IT Strategy and other Council Policies, as well as technical standards. Such requests to purchase must be based upon a User Requirements Specification document and take account of longer term organisational business needs.
2. Except for minor purchases, hardware must be purchased through the Council's procurement process
3. All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations are to be circulated for comment to all interested parties, well in advance of installation
4. All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment

UPS and power generators

1. An Uninterruptible Power Supply (UPS) is to be installed on all critical equipment to ensure the continuity of services during power outages
2. Secondary and backup power generators are to be employed where necessary to ensure the continuity of services during power outages

Using Fax Machines / Fax Modems

1. Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible. Both the owner of the information and the intended recipient must authorise the transmissions beforehand.
2. Sensitive or confidential information may only be sent via public telephone lines where more secure methods of transmission are not feasible. Both the owner of the information and the recipient must authorise the transmission beforehand

Using Centralised, Networked or Stand-Alone Printers

1. Information of a sensitive nature must not be sent to unattended printers.

Installing and Maintaining Network Cabling

1. Network cabling must be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall mounted sockets.
2. Any unused network wall sockets should be sealed-off or de-activated and their status formally noted

Consumables

1. IT Consumables must be purchased in accordance with the Council's approved purchasing procedures with usage monitored to discourage theft and improper use
2. Only personnel who are authorised to install or modify software shall use removable media to transfer data to / from the Council's network. Any other persons shall require specific authorisation

Working Off Premises or Using Outsourced Processing

1. Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable companies that operate in accordance with quality standards which should include a suitable Service Level Agreement which meets the Council's requirements.
2. Line management must authorise the issue of portable computers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices
3. Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.
4. Off-site computer usage, whether at home or at other locations, may only be used with the authorisation of line management. Usage is restricted to business purposes, and users must be aware of and accept the terms and

conditions of use, which must include the adoption of adequate and appropriate information security measures
5. Any movement of hardware between the Council locations is to be strictly controlled by authorised personnel
6. Personnel issued with mobile phones by the Council are responsible for using them in a manner consistent with the confidentiality level of the matters being discussed.
7. Personnel using alternative business premises to work on the Council's business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business premises systems.
8. Laptop computers are to be issued to, and used only by, authorised employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times

Using Secure Storage

1. Sensitive or valuable material and equipment must be stored securely and according to the value/ status of the equipment/ information being stored.
2. Documents and computer media are to be stored in a secure manner in accordance with their status. This may extend to lockable filing cabinets through to fire proof safes.

Documenting Hardware

1. Hardware documentation must be kept up-to-date and readily available to the staff who are authorised to support or maintain systems
2. A formal hardware inventory of all equipment is to be maintained and kept up to date at all times

Other Hardware Issues

1. Equipment owned by the Council may only be disposed of by authorised personnel who have ensured that the relevant security risks have been mitigated.
2. All information system hardware faults are to be reported promptly and recorded in a hardware fault register
3. All computing equipment and other associated hardware belonging to the Council must carry appropriate insurance cover against hardware theft, damage, or loss
4. All portable computing equipment is to be insured to cover travel domestically or abroad
5. All users of workstations, PCs / laptops are to ensure that their screens present an appropriate screen saver image when not being used
6. Approved login procedures must be strictly observed and users leaving their screen unattended must ensure access to their workstation is locked - or log off
7. Sensitive or confidential information must not be recorded on Answering Machine / Voice Mail systems
8. Only authorised personnel are permitted to take equipment belonging to the Council off the premises; they are responsible for its security at all times.

9. All equipment owned, leased or licensed by the Council must be supported by appropriate maintenance facilities from qualified engineers
10. Only suitable and approved cleaning materials are to be used on keyboards and screens owned by the Council
11. Deliberate or accidental damage to Council property must be reported to the nominated Information Security Officer as soon as it is noticed

Responsibilities:
All who use our computers and computer networks:

- You must make all requests for the purchase of hardware and associated equipment, (this includes trial equipment) using IT Services.
- You must have approval of your line manager before making the request to IT Services.
- Approval will only be granted for such purchases where there is a valid business reasons given.
- You must not install computer or any related equipment without the express consent of IT Services.

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management..
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of project managers:

- For any project, which involves new or upgraded equipment you are responsible for making sure the project produces a Equipment Purchasing Statement setting out the necessary purchasing requirements. The Head of IT must sign off this statement.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.
- The Head of IT, in conjunction with the Corporate Purchasing Team, is also responsible for introducing a procurement process, which will help us to enforce this policy.
- IT Services are responsible for the maintenance of a hardware inventory.
- IT Services are responsible the maintenance of a hardware fault register.
- IT Services are responsible recording and tracking any hardware warranties associated with computer and related equipment.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and

take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to prevent the purchase of unauthorised computer equipment and other related items. These controls will include:

Hardware Asset Management: IT Services will maintain an inventory of all hardware held by the Council.

Random Audits: IT Services will conduct random audits of the Council's computers, including portables PC's, printers, mobile telephones or any other equipment covered by this policy to ensure that no unauthorised products are in use. Audits may be conducted using an automatic auditing software product. The full co-operation of all users is required during audits.

Invoice Audits: IT Services, in conjunction with Audit Services and the Corporate Purchasing Team, will monitor the purchases made by Directorates.

Description	Controlling e-Commerce Information Security
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the use of e-commerce sites within the Council. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that e-commerce sites will be able to be deployed but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
E-Commerce Issues

1. e-commerce processing systems including the e-commerce Web site(s) are to be designed with protection from malicious attack given the highest priority.
2. e-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required.
3. The Council's e-commerce Web site(s) must be configured carefully by IT Staff to ensure that the risk from malicious intrusion is not only minimised but that any data captured on the site, is further secured against unauthorised access using a combination of robust access controls and encryption of data.
4. Where third parties are involved in e-commerce systems and delivery channels, it is essential that they are able to meet the resilience and Information Security objectives of the Council.

Responsibilities:
All who use our computers and computer networks:

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Processing Information and Documents
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the processing of information and documents. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that will enable processing and information may take place to the fullest extent but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
Networks
1. The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.
2. Suitably qualified staff are to manage the Council's network, and preserve its integrity in collaboration with the nominated individual system owners
3. Remote access to the Council's network and resources will only be permitted providing that authorised users are authenticated, data is encrypted across the network, and privileges are restricted.
4. System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion

System Operations and Administration
1. The Council's systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems.
2. System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the Council. In addition, they must be knowledgeable and conversant with the range of Information Security risks which need to be managed
3. For authorised personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy

4. Third party access to corporate information is only permitted where the information in question has been ‘ring fenced’ and the risk of possible unauthorised access is considered to be negligible
5. The management of electronic keys to control both the encryption and decryption of sensitive messages or processes must be performed under dual control, with duties being rotated between staff
6. The Council's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the Council’s information security.
7. System documentation is a requirement for all the Council’s information systems. Such documentation must be kept up-to-date and be available.
8. Error logs must be properly reviewed and managed by qualified staff
9. Systems Operations schedules are to be formally planned, authorised and documented.
10. Changes to routine systems operations are to be fully tested and approved before being implemented
11. Operational audit logs are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information system
12. System clocks must be synchronised regularly especially between the Council's various processing platforms."
13. Only qualified and authorised staff or approved third party technicians may repair information system hardware faults.
14. Transaction and processing reports should be regularly reviewed by properly trained and qualified staff.
15. Any external company utilised by the Council must be able to demonstrate compliance with this Council’s Information Security Policies and also provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance

<u>E-mail and the Worldwide Web</u>

1. Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material.
2. The transmission of sensitive and confidential data is to be authenticated by the use of digital signatures whenever possible.
3. E-mail should only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment of data files to an e-mail is only permitted after confirming the sensitivity of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.
4. Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code.
5. Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all staff.
6. Persons responsible for setting up Intranet access must ensure that any access restrictions pertaining to the data in source systems, are also applied to access from the Council’s Intranet.

7. Persons responsible for setting up Internet access are to ensure that the Council's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Resources management must ensure that all personnel with Internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet in addition to compliance with the Council's Information Security Policies
8. Due to the significant risk of malicious intrusion from unauthorised external persons, Web sites may only be developed and maintained by properly qualified and authorised personnel
9. Unsolicited e-mail is to be treated with caution and not responded to.
10. Ensure that information you are forwarding by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons.
11. Management is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents.
12. Staff authorised to make payment by credit card for goods ordered on the Internet, are responsible for its safe and appropriate use.
13. Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. Management must ensure that staff are made aware of the appropriate settings for the software concerned.
14. Information obtained from Internet sources should be verified before used for business purposes.
15. The Web site is an important marketing and information resource for the Council, and its safety from unauthorised intrusion is a top priority. Only qualified authorised persons may amend the Web site with all changes being documented and reviewed.
16. The Council will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by staff. Reports of attempted access will be scrutinised by management on a regular basis.
17. Computer files received from unknown senders are to be deleted without being opened.

<u>Telephones & Fax</u>

1. Conference calls are only permitted if staff are aware of the Information Security issues involved.
2. Video conference calls are only permitted if staff are aware of the Information Security issues involved.
3. All parties are to be notified in advance whenever telephone conversations are to be recorded.
4. Any fax received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission.
5. Staff authorised to make payment by credit card for goods ordered over the telephone, are responsible for safe and appropriate use.
6. The identity of recipients of sensitive or confidential information over the telephone must be verified.

7. The identity of persons requesting sensitive or confidential information over the telephone must be verified, and they must be authorised to receive it.
8. Unsolicited or unexpected faxes should be treated with care until the sender has been identified.

Data Management

1. Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques.
2. Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need.
3. The integrity and stability of the Council's databases must be maintained at all times.
4. Emergency data amendments may only be used in extreme circumstances and only in accordance with emergency amendment procedures.
5. The use of removable media disks e.g. disks and CD-ROMs is not permitted except where specifically authorised.
6. Data directories and structures should be established by the owner of the information system with users adhering to that structure. Access restrictions to such directories should be applied as necessary to restrict unauthorised access.
7. Existing directory and folder structures may only be amended with the appropriate authorisation, usually from the owner of the information system concerned
8. The archiving of documents must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff
9. The information created and stored by the Council's information systems must be retained for a minimum period that meets both legal and business requirements.
10. The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial / data models used for decision making are to be fully documented and controlled by the information owner.
11. Databases must be fully tested for both business logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature, procedures and access controls must ensure compliance with necessary legislation e.g. Data Protection
12. Highly sensitive or critical documents must not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports must be self contained and contain all the necessary information
13. Draft reports should only be updated with the authority of the designated owner of the report.
14. Draft version(s) of reports must be deleted or archived following production of a final version. A single version of the file should be retained for normal operational access.

15. Version control procedures should always be applied to documentation belonging to the Council or its customers.
16. Only authorised persons may access sensitive or confidential data on projects owned or managed by the Council or its employees.
17. The naming of the Council's data files must be meaningful and capable of being recognised by its intended users.
18. A document's title and ownership should be stated within the header and footer space on each page of all documents.
19. Temporary files on users' PCs and laptops are to be deleted regularly to prevent possible misuse by possible unauthorised users.
20. All users of information systems whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction.

Backup, Recovery and Archiving

1. Information system owners must ensure that adequate back up and system recovery procedures are in place.
2. Information and data stored on Laptop or portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.
3. Backup of the Council's data files and the ability to recover such data is a top priority. Management are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.
4. The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.
5. The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements.
6. Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files.

Document Handling

1. Hard copies of sensitive material must be protected and handled according to the distribution and authorisation levels specified for those documents.
2. All employees to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are highly sensitive.
3. All information used for, or by the Council, must be filed appropriately and according to its sensitivity.
4. Documents should be countersigned (either manually or electronically) to confirm their validity and integrity; especially those which commit or oblige the Council in its business activities.

5. Documents should be checked to confirm their validity and integrity; especially those which commit or oblige the Council in its business activities.
6. All written communications sent out by the Council to third parties are to be approved by authorised persons.
7. All signatures authorising access to systems or release of information must be properly authenticated.
8. Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified.
9. An agreed 'corporate' document style should be used which promotes consistency, integrity and promotes the agreed 'image' of the Council.
10. The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability, during and after transportation / transmission, are adequate and appropriate.
11. All documents of a sensitive or confidential nature are to be shredded when no longer required. The document owner must authorise or initiate this destruction.
12. All users of information systems must manage the creation, storage, amendment, copying and deletion / destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary will be applied by management and determined by the classification of the information / data in question.

<u>Securing Data</u>

1. Where appropriate, sensitive or confidential information or data should always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques.
2. Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the Council and to external parties.
3. Prior to sending information to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and Information Security measures adopted by the third party, must be seen to continue to assure the confidentiality and integrity of the information.
4. Information relating to the clients and third party contacts of the Council is confidential, and must be protected and safeguarded from unauthorised access and disclosure
5. Customer credit card details entrusted to the Council must be afforded a combination of security measures (technology and procedural) which, in combination, prevent all recognised possibilities of the card details being accessed, stolen, modified or an any other way divulged to unauthorised persons.

6. All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and sensitivity of the information being safeguarded.
7. Prior to sending reports to third parties, not only must the intended recipient(s) be authorised to receive such information, but the procedures and Information Security measures adopted by each third party, must be seen to continue to assure the confidentiality and integrity of the information.
8. Sensitive financial information must be afforded security measures (technology and procedural) which, in combination, safeguard such information from authorised access and disclosure.
9. Data created or owned by others is to be protected against unauthorised or accidental changes, and may only be deleted with the proper authority.
10. Sensitive / confidential electronic data and information should be secured, whenever possible, with access control applied to the directory on the (computer) system concerned. The sole use of passwords to secure individual documents is less effective, and hence discouraged, as passwords may be either forgotten or become revealed (over time) to unauthorised persons
11. Information classified as sensitive may never be sent to a network printer without there being an authorised person to retrieve it and hence safeguard its confidentiality during and after printing.

<u>Other Information Handling and Processing</u>

1. The decision whether dual control is required for data entry is to be made by the information system owner. Where so required, secure data handling procedures including dual input are to be strictly adhered to.
2. Employees are not permitted to load non-approved screen savers onto the Council's PCs, laptops and workstations.
3. Any third party used for external disposal of the Council's obsolete equipment and material must be able to demonstrate compliance with this Council's Information Security Policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance.
4. The use of photocopiers or duplicators for personal use is discouraged. In exceptions, specific permission may be given by the employee's immediate supervisor or manager.
5. The techniques of dual control and segregation of duties are to be employed to enhance the control over procedures wherever both the risk from, and consequential impact of, a related Information Security incident would likely result in financial or other material damage to the Council.
6. This Council expects all employees to operate a clear desk policy in respect of sensitive and confidential files and documents.
7. E-mail addresses and faxes are to be checked carefully prior to dispatch, especially where the information is considered to be confidential; and where the disclosure of the e-mail addresses or other contact information, to the recipients is a possibility.
8. The Council values the integrity and correctness of all its business and related information and requires management to develop and adopt the appropriate procedures in this regard.

9. Employees travelling on business are responsible for the security of information in their custody.

Responsibilities:
All who use our computers and computer networks:

- Need to understand the duties and responsibilities that this policy imposes on them.

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Purchasing and Maintaining Commercial Software
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the purchasing and maintenance of commercial software. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that will enable the purchase and maintenance of commercial softrware to take place to the fullest extent but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:

Purchasing and Installing Software

1. All requests for new applications systems or software enhancements must be presented to the Information Systems Group with a Business Case with the business requirements presented in a User Requirements Specification document.
2. The Council should generally avoid the selection of business critical software which has not been adequately proven by early adopters of the system. The selection process for all new business software must additionally incorporate the criteria upon which the selection will be made. Such criteria must receive the approval of the project board.
3. All office software packages must be compatible with the Council's preferred and approved computer operating system and platforms and conform to the Council's ICT Strategy.
4. To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User Licence Agreements are to be strictly adhered to
5. The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased Information Security risks associated with such projects are mitigated using a combination of procedural and technical control techniques.

Software Maintenance & Upgrade

1. Patches to resolve software bugs may only be applied where verified as necessary and with authorisation from the IT Unit. They must be from a reputable source and are to be thoroughly tested before use.

2. Upgrades to software must be properly tested by qualified personnel before they are used in a live environment.
3. The decision whether to upgrade software is only to be taken after consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and necessity for such change
4. Developing Interfacing software systems is a highly technical task and should only be undertaken in a planned and controlled manner by the IT Unit
5. All application software must be provided with the appropriate level of technical support to ensure that the Council's business is not compromised by ensuring that any software problems are handled efficiently with their resolution available in an acceptable time.
6. Necessary upgrades to the Operating System of any of the Council's computer systems must have the associated risks identified and be carefully planned, incorporating tested fall-back procedures. All such upgrades being undertaken as a formal project.
7. Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to
8. Software faults are to be formally recorded and reported to the IT Service Desk for software support / maintenance.

Other Software Issues

1. The disposal of software should only take place when it is formerly agreed by the user that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.

Responsibilities:

All who use our computers and computer networks:

- Need to understand the duties and responsibilities that this policy imposes on them.

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Developing and Maintaining In House Software
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the development and maintenance of in-house software. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that will enable the development and maintenance of in-house software to take place to the fullest extent but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
Controlling Software Code

1. Only designated staff may access operational program code libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control.
2. Only designated staff may access program source libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control.
3. Formal change control procedures must be utilised for all changes to systems. All changes to programs must be properly authorised and tested before moving to the live environment
4. Program listings must be controlled and kept fully up to date at all times.
5. Formal change control procedures with comprehensive audit trails are to be used to control program source libraries
6. Formal change control procedures with comprehensive audit trails are to be used to control versions of old programs

Software Development

1. Software developed for or by the Council must always follow a formalised development process which itself is managed under the project in question. The integrity of the Council's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.
2. Emergency amendments to software are to be discouraged, except in circumstances previously designated by senior management as

'critical'. Any such amendments must strictly follow agreed change control procedures.

3. All proposed system enhancements must be business driven and supported by an agreed Business Case. Ownership (and responsibility) for any such enhancements will initially rest with the business owner of the system with final approval residing with the Information Systems Group.
4. The development of bespoke software is only to be considered, if warranted by a strong Business Case and supported both by management the Information Systems Group.
5. Formal change control procedures must be utilised for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment.
6. IT Managers must ensure that proper segregation of duties applies to all areas dealing with systems development, systems operations, or systems administration.

Testing & Training

1. Formal change control procedures must be employed for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment.
2. The use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place.
3. Formal change control procedures must be utilised for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment.
4. New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the Council.
5. Normal system testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. The results of parallel running should not reveal problems or difficulties which were not previously passed during user acceptance testing.
6. Training is to be provided to users and technical staff in the functionality and operations of all new systems.

Documentation

1. All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

Other Software Development

1. Third party developed software must meet the user requirements specification and offer appropriate product support.

Responsibilities:
All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Combating Cyber Crime
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the development and maintenance of in-house software. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that will enable the development and maintenance of in-house softrware to take place to the fullest extent but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:

Combating Cyber Crime

1. Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimise the threats from cyber crime.
2. Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cyber crime attacks can be minimised and that restoration takes place as quickly as possible.
3. Perpetrators of cyber crime will be prosecuted by the Council to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence.
4. In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times."
5. It is a priority to minimise the opportunities for cyber crime attacks on the Council's systems and information through a combination of technical access controls and robust procedures.
6. Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy.
7. Risks to the Council's systems and information are to be minimised by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices.
8. Procedures to deal with hoax virus warnings are to be implemented and maintained.

9. Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across both servers, PCs and laptop computers.
10. The threat posed by the infiltration of a virus is high, as is the risk to the Council's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested.

Responsibilities:
All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Complying with Legal & Policy Requirements
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the observance of some of the many legal obligations that staff and the Council are under a duty to observe in the area of IT. It is by no means a comprehensive list but does cover some of the most common areas. It also details the controls that need to be in place to ensure these are properly observed.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
Complying with Legal Obligations

1. All staff are to be made fully aware of their legal responsibilities with respect to their use of computer based information systems and data.
2. The Council and staff will fully comply with the requirements of Data Protection legislation and the Freedom of Information Act.
3. All staff are to be made fully aware of the key aspects of Copyright, Designs and Patents Act legislation in so far as these requirements impact on their duties.
4. All staff are to be made fully aware of the key aspects of Software Copyright and Licensing legislation, in so far as these requirements impact on their duties.
5. All staff are to be made fully aware of the key aspects of Computer Misuse legislation, in so far as these requirements impact on their duties.

Complying with Policies

1. The Council will maintain a suitable archiving and record retention procedure.
2. All employees are required to fully comply with the Council's Information Security policies. The monitoring of such compliance is the responsibility of the Council's Information Officer.

Avoiding Litigation

1. Employees are prohibited from writing derogatory remarks about other persons or organisations.
2. Information from the Internet or other electronic sources may not be used without authorisation from the owner of the copyright.

3. Information from the Internet or other electronic sources may not be retransmitted without permission from the owner of the copyright.
4. Text from reports, books or documents may not be reproduced or reused without permission from the copyright owner.

Other Legal Issues

1. All staff are to be made fully aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer.
2. Registered domain names, whether or not actually used for the Council's Web sites, are to be protected and secured in a similar manner to any other valuable asset of the Council.
3. A re-assessment of the threats and risks involved relating to the Council's business activities must take place periodically to ensure that the Council is adequately insured at all times.
4. All parties are to be notified in advance whenever conversations are being recorded

Responsibilities:

All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:

The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Planning for business continuity
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern business continuity planning. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that will enable business continuity planning to take place to the fullest extent but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:

Business Continuity Management (BCP)

1. A Business Continuity Plan it to be initiated.
2. A formal risk assessment is to be undertaken in order to determine the requirements for a Business Continuity Plan.
3. A Business Continuity Plan is to be developed which covers all essential and critical business activities.
4. All staff and managers must be made aware of the Business Continuity Plan and their own respective roles.
5. The Business Continuity Plan is to be periodically tested to ensure that all managers and staff understand how it is to be executed.
6. The Business Continuity Plan is to be kept up to date and re-tested periodically.

Responsibilities:
All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.

- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:

The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Addressing Personnel Issues Relating to Security
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern certain HR aspects relating to the use of Council IT equipment and systems. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that staff will be aware of their obligations and the boundaries when working in this environment. It will enable then to act and behave in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:

1. All staff are to be reminded of the requirements for compliance with this Information Security policy.
2. All external suppliers who are contracted to supply services to the organisation must agree to follow the Information Security policies of the Council. An appropriate summary of the Information Security Policies must be formally delivered to any such supplier, prior to any supply of services.
3. The organisation's letter-headed notepaper, printed forms and other documents are to be handled securely to avoid misuse.
4. The lending of keys, both physical or electronic, is prohibited.
5. All staff are to be reminded of the need to protect the confidentiality of information, both during and after their employment with the Council.
6. Notwithstanding the organisation's respect for employee's privacy in the workplace, it reserves the right to have access to all information created and stored on the organisation's systems.
7. All employee data is to be treated as strictly confidential and made available to only properly authorised persons.
8. All IT staff must have previous employment and other references carefully checked.
9. Employees may not use the organisation's systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardises security. All Internet use during core hours must be for business related purposes
10. All staff will have the Council's Internet usage policy brough to their attention when they access the Internet.
11. All staff must treat passwords as private and highly confidential.

12. Confidential information should be shared only with other authorised persons. Non-compliance with this policy could result in disciplinary action.
13. The use of e-mail for personal use is discouraged, and should be kept to a minimum. Postal mail may be used for business purposes only.
14. Personal calls on the telephone systems are to be minimised and limited to urgent or emergency use only. The cost of all personal calls needs to be repaid to the Council.
15. The use of the organisation's mobile and desk phones will to be monitored for inappropriate call patterns, unexpected costs, and excessive personal use.
16. 'Company' Credit cards issued to authorised staff remain the responsibility of those employees until the card is returned or cancelled.
17. All staff need to be informed that telephone or e-mail enquiries for sensitive or confidential information are initially to be referred to their line managers. Only authorised persons may disclose information of this nature, and then only to persons whose identity and validity to receive such information has been confirmed
18. All data and information not in the public domain, relating to the Council's business and its employees, must remain confidential at all times. Such information must not be discussed outside work, with family members or on the "grapevine" at work.
19. The playing of games on office PCs or laptops is prohibited.
20. Using the Council's computers for personal / private business is prohibited.
21. Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Information Security Officer
22. Upon notification of staff resignations, HR must consider with their staff's line manager and the appointed Information Security Officer whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights.
23. Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges

Responsibilities:

All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use

our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:
- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Controlling e-Commerce Information Security
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the use of e-commerce sites within the Council. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that e-commerce sites will be able to be deployed but in a manner that is secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
E-Commerce Issues

1. e-commerce processing systems including the e-commerce Web site(s) are to be designed with protection from malicious attack given the highest priority.
2. e-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required.
3. The Council's e-commerce Web site(s) must be configured carefully by IT Staff to ensure that the risk from malicious intrusion is not only minimised but that any data captured on the site, is further secured against unauthorised access using a combination of robust access controls and encryption of data.
4. Where third parties are involved in e-commerce systems and delivery channels, it is essential that they are able to meet the resilience and Information Security objectives of the Council.

Responsibilities:
All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Premises Security
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the use of premises to host IT equipment and facilities for the Council. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such a way that premises are secure and minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
Premises Security

1. The sites chosen to locate computers and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards.
2. Computer premises must be safeguarded against unlawful and unauthorised physical intrusion.
3. When locating computers and other hardware, suitable precautions are to be taken to guard against the environmental threats of fire, flood and excessive ambient temperature / humidity.
4. All computer premises must be protected from unauthorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts.
5. All employees are to be aware of the need to challenge strangers on the organisation's premises.

Data Stores

1. On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level.
2. Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level

Other Premises Issues

1. The security of network cabling must be reviewed during any upgrades or changes to hardware or premises.

2. Owners of the organisation's information systems must ensure that disaster recovery plans for their systems are developed, tested, and implemented."

Responsibilities:
All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.

Description	Detecting and Responding to IS Incidents
Author	John Nutley
Version	1.0
Approval Date	Draft

Purpose:
The aim of this annex is to state the principles that will govern the response when IS incidents are dectected and guidance on the correct action to take. It also details the controls that need to be in place to ensure these are properly observed. These principles are designed in such that the responses to the detection and subsequent corrective action minimises the exposure of the Council to any security breach or loss of data.

Scope:
This policy applies to all councillors, employees, contractors, volunteers, suppliers or other agents who have access to our computers or computer networks.

Policy Principles:
Reporting Information Security Incidents

1. All suspected Information Security incidents must be reported promptly to the appointed Information Security Officer.
2. Information Security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorised persons.
3. Any Information Security breaches must be reported without any delay to the appointed Information Security Officer to speed the identification of any damage caused, any restoration and repair and to facilitate the gathering of any associated evidence.
4. All identified or suspected Information Security weaknesses are to be notified immediately to the Information Security Officer.
5. Persons witnessing Information Security incidents or breaches should report them to the Information Security Officer without delay.
6. Employees are expected to remain vigilant for possible fraudulent activities.

Investigating Information Security Incidents

1. Information Security incidents must be properly investigated by suitably trained and qualified personnel.
2. Evidence relating to an Information Security breach must be properly collected and forwarded to the Information Security Officer.
3. Evidence relating to a suspected Information Security breach must be formerly recorded and processed.
4. The Information Security Officer must respond rapidly but calmly to all Information Security incidents, liaising and coordinating with colleagues to both gather information and offer advice.

Corrective Activity

1. A database of Information Security threats and ‘remedies’ should be created and maintained. The database should be studied regularly with the anecdotal evidence used to help reduce the risk and frequency of Information Security incidents in the Council.

Other Information Security Incident Issues

1. The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations.
2. Information Security incidents arising from system failures are to be investigated by competent technicians.
3. Breaches of confidentiality must be reported to the Information Security Officer as soon as possible.
4. During the investigation of Information Security incidents, dual control and the segregation of duties are to be included in procedures to strengthen the integrity of information and data.
5. Staff shall be supported by management in any reasonable request for assistance together with practical tools, such as security incident checklists, etc., in order to respond effectively to an Information Security incident.
6. Information relating to Information Security incidents may only be released by authorised persons.

Responsibilities:

All who use our computers and computer networks:-

- Need to understand the duties and responsibilities that this policy imposes on them

Additional responsibilities of the Chief Executive, Directors, Heads of Service and line managers:

- You are responsible for making sure that you, your staff and any contractors, volunteers or other agents under your supervision who use our computers or computer networks know about, understand and keep to this policy.
- If you are a line manager, you will need to actively manage the control standards which are in place for the systems under your management.
- Where an infringement of this policy has been identified and rectified the appropriate Directorate will meet any additional or unexpected costs.

Extra responsibilities of IT Services:

- The Head of IT is responsible for preparing and updating this policy.

If any person fails to keep to this policy, the Head of Information Services, the Head of Legal Services and the Head of Audit will investigate the matter and

take the appropriate action. The action taken will depend on particular circumstances but could result in:

- Disciplinary action, including dismissal for employees.
- Loss of contract and fines for contractors or agents.
- The matter being referred to the Standards Committee for Councillors.

Enforcement:
The Council reserves the right to protect its reputation and its investment by enforcing strong internal controls to ensure the policy principles laid out in this annex are adhered to. These controls will include:

Random Audits: Audit Services will conduct regular audits on key systems to ensure that all controls are in place and are being monitored by system owners. The full co-operation of all users is required during audits.