INFORMATION SECURITY POLICY

Version 1.0

December 2014

ICT Shared Services

Forest of Dean District Council

Cheltenham Borough Council

ubico

CBH

GO Shared Services

Forest of Dean District Council In partnership with Gloucester City Council and Civica

Cheltenham Leisure and Culture Trust

Contents

Scope of the Policy

Forest of Dean District Council (FoDDC) is the lead authority in a Shared Service (ICTSS) for the delivery of ICT services with Cheltenham Borough Council (CBC). Users of the ICT Shared Service include Cheltenham Borough Homes, Cheltenham Trust, Ubico and part of GO Shared Services.

This policy has been developed to take on the needs of all the ICT users in terms of information security and covers both paper and electronic information. It applies to all ICT users including Members and Contractors. It is the responsibility of everyone to ensure they read and understand their obligations under it.

This policy should be read in conjunction with the ICTSS Acceptable Usage Policy and Personal Commitment Statement signed by all staff. Please be aware there may be local organisational policies that extend this policy further.

Policy Objectives

The objectives of this Policy are to:

- Communicate to all ICT users the position on information security.
- Define the expectations on all ICT users, with regard to the secure use of information and business assets.
- Demonstrate best endeavours to address information security threats

Security Working Groups

The Shared Service has established a joint Security Working Group (SWG). This group is chaired by FoDDC Head of Paid Service who is also ICTSS Senior Information Risk Owner (SIRO).FoDDC will also provide resources, accommodation and administrative support for the group. The joint SWG is responsible for all aspects of ICT security across the Shared Service. It reports to the Shared Service SIRO, the CBC SIRO and where required, the Public Services Network Accreditation Panel (PSNAP), and meets at regularintervals.

Further details on the SWG can be found in the Public Service Network Connection Compliance Terms of Reference document which also details the individual security officer roles.

What is information security?

Information security is being responsible about information we hold. It is about safeguarding the information (data), making sure it is; current (up to date), correct (we have accurate records), is kept confidential (only authorised parties can access the information) and it is available (it can be accessed when necessary).

It is also about the physical security of our equipment, technical infrastructure and buildings and making sure that unauthorised people do not have access to it.

Why is information security important?

Information (data) can be stored in various ways on various media (even the recording of a voice on tape). It can be stored electronically/magnetically on equipment. It can also be printed or written.

We often think of security as someone else’s responsibility and it is only when it affects us personally that we take it seriously. For example if we were unable to use our computers at work because a virus had infected the network, or if we found a fraudulent transaction on our bank statement. Just as banks and building societies have an obligation to keep information about us safe we too have a duty to keep the information we hold about our customers safe.

There are legal and financial implications of not keeping information that is accurate and appropriately protected. It is also important to realise that good data management and security helps us to provide high quality services.

Information Security Principles

In meeting its Information Security responsibilities the ICTSS has adopted the four key principles described by Her Majesty’sGovernment (HMG):

Principle 1: **ALL**information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

Principle 2: **EVERYONE** who works with government (including staff, elected members, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

Principle 3: Access to **sensitive** information must **ONLY** be granted on the basis of a genuine ’need to know’ and an appropriate personnel security control.

Principle 4: Assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

The following basic principles should be used:

- Handle with care to avoid loss, damage or inappropriate access
- Share responsibly, for business purposes only
- Store assets securely when not in use
- Where assets are taken outside the office environment they should be protected in transit, not left unattended and stored securely

- Prevent overlooking or inadvertent access when working remotely or in public places
- When discussing business in public or by telephone, appropriate discretion should be exercised
- Report any incidents involving theft, loss or inappropriate access

Industry standard ISO 27001

ISO 27001 is a specification for the management of Information Security. It is applicable to all sectors of industry and commerce and not confined to information held on computers. It addresses the security of information in whatever form it is held. This is a standard that ICTSS aspire to.

Confidentiality

All ICT users and those that have access to OFFICIAL and OFFICIAL-SENSITIVE documents are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If anyone is unsure of whether they should pass on information, they should consult the appropriate Service manager or their legal advisor

All ICT users must make every effort to ensure that where appropriate the confidentiality of email is maintained. ICT usersshould be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over external networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of ICTSS.

Care should be taken when addressing all emails, but particularly where they include OFFICIAL – SENSITIVE information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) is not permitted and has been disabled at a system level. Please consult the ICTSS Service Desk if there is a specific business requirement.

Data Classification

All routine public sector business, operation and services should be treated as OFFICIAL and all organisations on the ICTSS Network operate exclusively at this level.

Examples of OFFICIAL information include:

- The day-to-day business of the Council, including information about public services and finances
- Public safety, criminal justice and law enforcement
- Commercial information, including contractual information and intellectual property
- Personal information that is required to be protected under the Data Protection Act

There is no requirement to mark OFFICIAL information, although it is recommended that when emailing any Personal Information that is required to be protected under the Data Protection Act then the email should identify that the information should be treated in accordance with the provisions of the Data Protection Act.

A sub-set of OFFICIAL information is OFFICIAL-SENSITIVE and information which falls within this category should be marked accordingly.

Information which falls within the category of OFFICIAL-SENSITIVE includes:

- The most sensitive corporate information, such as organisational restructuring, negotiations and major security or business continuity issues
- Very sensitive personal information, such as information about vulnerable or at-risk people or private financial information
- Commercial or market sensitive information
- Information about investigations and civil or criminal proceedings that could disrupt law enforcement or prejudice court cases

If you have been issued with a laptop or other portable device, or you are handling OFFICIAL-SENSITIVE files, you must ensure that they are locked away when unattended; you must also ensure you are not being overlooked when working on such files.

ICT users must never leave any such information or devices unattended in public areas, anywhere where they maybe accessed by non-ICT users or on display i.e. in the back of a car or on a printer.

Document Marking

There is no requirement to mark documents which contain OFFICIAL information. However, security classifications must be added to all documents which contain OFFICIAL-SENSITIVE information.

The following scheme has been adopted for marking OFFICIAL – SENSITIVE information:

Email: OFFICIAL-SENSITIVE must appear in the subject line of the email. This can be done by selecting the appropriate remote button when sending the email

Word/Excel: The words OFFICIAL-SENSITIVEmust appear in the header and footer of the document

Folders/binders: The words OFFICIAL-SENSITIVE must appear on the front of the folder

Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.

The equipment must not be moved or modified by anyone without authorisation from the ICT Service Desk.

All computer equipment must be supplied, configured and connected by ICTSS. Users must not bring in devices and attach or connect them to Council equipment or the network; existing devices supplied by ICTSS must not be reconnected or reconfigured by the User.

Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

Equipment Maintenance

ICTSSmust ensure that all IT equipment is maintained in accordance with the manufacturer’s instructions and with any documented internal procedures to ensure it remains in working order.

Staff involved with maintenance should:

- Retain all copies of manufacturer’s instructions.
- Identify recommended service intervals and specifications.
- Enable a call-out process in event of failure.
- Ensure only authorised technicians complete any work on the equipment.
- Record details of all remedial work carried out.
- Identify any insurance requirements.
- Record details of faults incurred and actions required.

A service history record of equipment should be maintained so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

Equipment maintenance must be in accordance with the manufacturer’s instructions. This must be documented and available for support staff to use when arranging repairs.

Security of Equipment – Off Premises

The use of equipment off-site must be formally approved by the user’s Line Manager. Equipment taken away from Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted if carrying OFFICIAL-SENSITIVE information
- Be password protected.
- Be adequately insured.

Users should ensure, where necessary that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the ICTSS.

Staff should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act.

Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools. All IT equipment must be returned to the ICTSS for data removal.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

Accessing ICT systems

If you require access to any ICT system you will be issued with a username and password which you will use every time you log onto a computer; this username and password is unique and confirms your identity.

All actions on the network are logged under the username that carried them out and therefore if someone else uses your username and password to carry out transactions it would be difficult to prove that it was not you.

A poorly chosen password creates a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include all single words from the dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- at least seven characters (ICT Administrators with Domain Administrator privileges must use a 14 character password)
- one or more numerical digits
- more complex than a single word
- one or more UPPERCASE characters and one or more lowercase characters

Please consider using a sentence or phrase as well as the standards above.

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- never reveal your password to anyone
- never use the remember password function
- never write your passwords down or store them where they are open to theft
- never store your passwords in a computer system without encryption
- do not use any part of your username in your password
- do not use the same password for systems inside and personal systems outside of work.

All passwords must be changed at a maximum of every 90 days, or whenever the system prompts you to change it. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately.

Users must not reuse the same password within 10 password changes.

Remote Access

Citrix Access Gateway is the primary method of connection for remote users. An individual wishing to connect remotely must have the authorisation from their line manager together with a description as to what services and functions they should be allowed to perform whilst working remotely. Individualsshould contact the ICTSSService Desk in order to discuss their requirements.

Although user-owned devices are permitted to remotely access the ICTSS network, these must be regularly patched and have an up-to-date antivirus/antimalware product installed. ICTSS reserve the right to disallow any remote computer failing the above test.

If access is required to the Public Services Network (PSN), a PSN Service or a corporate system that is linked to a PSN Service access MUST only be obtained via a corporately managed and approved device. A small pool of loan laptops is available from the ICTSS Service Desk if occasional use is needed for this function. For a more permanent solution, please discuss this with the ICTSS Service Desk.

All corporately managed laptops are encrypted and provided with power supplies and an appropriate protective case. The ICTSSis unable to support these machines off site, so they must be returned to the ICT Service Desk for support if a problem occurs. No data should be stored on these laptops as they are wiped after being returned to ICTSS.

The Council will not provide technical support for personal equipment used to connect to the Citrix Access Gateway. This includes routers, home broadband, cyber cafés, laptops, desktops, printers, etc.

Removable Media

All removable devices are prohibited unless there is a valid business case for their use. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

By default therefore, access to removable media will be disabled unless there is a valid business case that has been completed, signed-off by your line manager and ICTSS.

The policy of prohibiting access to removable media applies to (but is not restricted to) removable media listed below:

a) Bluetooth devices;
b) Media Cards;
c) CDs/DVDs (optical disks);
d) Digital cameras;
e) External Hard Drives;
f) PDA devices
g) Infrared devices;
h) Tape drives;
i) USB Memory Sticks (also known as pen drives or flash drives);
j) MP3 Players;
k) Audio Tapes (including Dictaphones and Answering Machines).

The following devices supplied by ICTSS will be enabled for all equipment by default:

a) Keyboards;
b) Mice;
c) Monitors;
d) Telephone headsets;

Requests for access to, and use of, removable media devices must be made to the ICTSS using the Removable Media Business Case form (**Appendix A**). Please talk to ICT for advice and guidance on completing this document, guidance notes are provided (Appendix B).

All Business Case applications will be approved by either the FoDDC or CBC Security Working Group or at FoDDC the Group Manager for Customer Services or CBC the Director of Resources.

It is important that the risks of using removable media are understood, and that appropriate reviews as to why a member of staff requires this access are carried out. All removable media authorisations willbe reviewed on an annual basis.

All removable media devices and any associated equipment and software must only be purchased and installed by ICTSS. No other removable media devices are to be used to store an organisation’s data, and must not be used with any ICTSSowned or leased IT equipment unless there is an approved business case for doing so.

In order to minimise risk of physical damage, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Virus and malware checking software is operational on all ICTSS managed equipment and will check all files on access. An up-to-date virus/malware software MUST be on any machine accessing a corporately owned device. Please contact ICTSS if you are in any doubt on any machine.

All ICTSS users can check corporately managed PC's to determine if this local software is working by looking at their at the desktop tool bar where there should be an icon that is green if the PC is safe (if you hover the curser over the icon it will say PC status protected) . If it is red then you should contact ICTSS.   Users should note that this does not apply to igel's.

Removable media devices that are no longer required, or have become damaged, must be returned to ICTSS and will be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the organisation or for external use, must be erased. All disposal or sanitisation must be carried out by a member of the ICTSS team or a reputable data disposal / sanitisation organisation.

Smartphones and Tablets

The use of personal smartphones and tablets are permitted for business use (e.g. linked to corporate email, corporate intranet and corporate documents) if they have been checked and approved by ICTSS.For an up-to-date list of supported devices please contact the ICTSS.

To ensure the security of information stored on smartphones and/or tablets security settings will be enabled to:

- Enforce password setting
- Ensure an minimum password length
- Automatically lock the device after 5 minutes of inactivity, and
- Remove all corporate content after 4 failed password attempts or in the event the personal device is lost or stolen.
- All software (e.g. Apps) on the device can be monitored
- All devices are not allowed to be hacked or Jail broken

Email

All emails that are used to conduct or support official business must be sent using the individual's allocated email address. Non-work email accounts **must not** be used to conduct or support official business.

Users must ensure that any emails containing sensitive information must be sent from an official email address. Any emails containing OFFICIAL-SENSITIVE information must be sent from a GCSx email. All emails that represent aspects of the organisation's business or organisation's administrative arrangements are the property of the organisationand not of any individual ICT User.

Emails held on ICTSS approved equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent should be considered to be an official communication from the individual organisations (Data Controllers). In order to ensure protection from misuse of e-mail, the following controls will be exercised:

All official external e-mail will carry the following disclaimer (which is added automatically):

> *"This email, and any attachments, may contain OFFICIAL or OFFICIAL-SENSITIVE information and is intended solely for the individual to whom it is addressed. It may contain sensitive or protectively marked material and should be handled accordingly. If this Email has been misdirected, please notify the author immediately.*
> *If you are not the intended recipient you must not disclose, distribute, copy, print or rely on any of the information contained in it or attached, and all copies must be deleted immediately. Whilst we take reasonable steps to try to identify any software viruses, any attachments to this Email may nevertheless contain viruses which our anti-virus software has failed to identify. You should therefore carry out your own anti-virus checks before opening any documents. This organisation will not accept any liability for damage caused by computer viruses emanating from any attachment or other document supplied with this e-mail. All traffic may be subject to recording and / or monitoring in accordance with relevant legislation."*

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, or that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or classified information or for communicating in the particular circumstances.

Email must not be considered to be any less formal than memos or letters that are sent out from a particular service. When sending external email, care should be taken not to include any material which would reflect poorly on the organisationsreputation or its relationship with customers, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate. Content filters are used to detect such material. Any user who is unclear about the appropriateness of any material should consult their Line Manager or the ICT Service Desk prior to commencing any associated activity or process.

IT facilities provided by the ICTSS for email should not be used for:

- the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind;
- the transmission of material that infringes the copyright of another person, including intellectual property rights;
- activities that unreasonably waste staff effort or use networked resources,
- activities that disrupt the work of other users;
- the creation or transmission of material which is designed or likely to cause annoyance, inconvenience, needless anxiety or discrimination;
- the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others;
- unfairly criticising individuals, including copy distribution to other individuals;
- the creation or transmission of material which brings the organisation into disrepute.

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the list can confirm the existence of an address following a speculative e-mail.

Before giving your email address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter emails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using ICTSSsystems or facilities.

All ICT users are provided with a limited mail box size of 250MB. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems. If you would like assistance with mailbox management contact the ICT Service Desk. There is an automated email Archiving system also in place to assist in managing your mailbox.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This should also be the preferred method of transferring OFFICIAL-SENSTIVE information. If a copy of a file must be sent then it should not exceed 20MB in size, if it does please contact the ICTSS service desk for advice on alternative methods of transmission.

All users should be aware that email usage can be monitored and recorded centrally to prevent inappropriate or offensive emails are not sent or received.

Monitoring of content will only be undertaken by staff specifically authorised for that purpose and with Information Asset Owner approval. These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters;
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities;
- Preventing or detecting crime;
- Investigating or detecting unauthorised use of email facilities;
- Ensuring effective operation of email facilities;
- Determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact the ICT Solutions Manager together with the approval of a Senior Manager within their organisation. Designated staff in the ICT Department can investigate and provide evidence and audit trails of access to systems. The ICT Department will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers Act for this information.

Access to another user's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. If this is the case a written request to the ICT Solutions Manager is required from a Senior Manager within the organisation. This access must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the employee. Managers must only open emails which are relevant to the business need for which this was granted.

All emails sent from and to @fdean.gov.uk, @fdean.gcsx.gov.uk, @cheltenham.gov.uk, @cheltenham.gcsx.gov.uk, @cheltborohomes.org, @ubico.co.uk, @westoxon.gov.uk, @westoxon.gcsx.gov.uk, @cotswold.gov.uk @cotswold.gcsx.gov.uk& @cheltenhamtrust are transmitted via secure data links.

Viruses/Malware

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the ICTSS Service Desk immediately.

In particular, users:

- Must unplug local devices immediately to prevent the spread of infection
- Must not transmit by email any file attachments which they know or suspect to be infected with a virus;
- Must not download data or programs of any nature from unknown sources;
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities;
- Must not forward virus warnings other than to the ICT Service Desk only when requested;
- Must report any suspected files to the ICTSSService Desk.

In addition, ICT will ensure that email is appropriately virus checked at the network boundary, and where appropriate will use two functionally independent virus checkers.

Software

Software acquisition channels are restricted to ensure that there is a complete record of all software that has been purchased and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet. For this reason, all software MUST be acquired by ICTSS.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be used as there is a serious risk of introducing a virus.

Software must be registered in the name of the organisation; Software will never be registered in the name of an individual.

The ICTSSmaintains a register of all software and will keep a library of software licenses. The register must contain:

a) The title and publisher of the software;
b) The date and source of the software acquisition;
c) The existence and location of back-up copies;
d) The software product's serial number;
e) Type of data being recorded.

Software on Local Area Networks or multiple machines shall only be used in accordance with the licence agreement and updated to the latest supported version.

Software must only be installed by the ICTSS once the registration requirements have been met. Once installed, the original media will be returned to the ICTSSand kept in a safe storage area maintained by the ICT Service Desk.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software without prior approval from the ICT Solutions Manager.

Software must not be changed or altered by any user unless there is a clear business need. All changes to software should be authorised before the change is implemented. A full procedure should be in place and should include, but not be limited to, the following steps:

- Change requests affecting a software asset should be approved by the software asset’s owner;
- All change requests should consider whether the change is likely to affect existing security arrangements and these should then be approved;
- A record should be maintained of agreed authorisation levels;
- A record should also be maintained of all changes made to software;

- Changes to software that have to be made before the authorisation can be granted should be controlled.

Application development

ICTSSdoes not generally undertake detailed application development, however, it is noted that:

- Interfacing projects to allow for data to transfer between internal systems are conducted.
- ICTSS are increasingly involved in provision of e-government facilities, which are likely to involve applications development.

This policy requests that security should be considered during the development of systems, both in relation to those developing the systems, and the security of the data stored.

An analysis of security issues should be carried out at an early stage in any development project. The security requirements should be consistent with this policy, and its family of documents. Resources and costs should be part of project assessment with agreed and assigned resources before any work is done.

Application development security requirements will typically address the following areas:

- Authentication (or user identification)
- Access controls
- Accounting and audit trail – the logging and monitoring of events.
- Communications security (e.g. encryption of data across networks)
- Integrity
- Availability

Additionally, industry standard good practice and methodology should form part of the development for example IEEE (Institute of Electrical and Electronics Engineers) and ISO.

Payment Card Industry (PCI) security standard

Credit and debit card payments – Compliance

The Data Protection Act and this Policy applies to the processing of credit and debit card payments and for the security of any personal data collected or held in relation to these payment processes.

If your service accepts payments from debit and credit cards then you are responsible for the security of any data collected or stored. These payments include Compliance with the PCI standard that includes protecting:

- Card readers
- Point of sale systems

- Store networks & wireless access routers
- Payment card data storage and transmission
- Payment card data stored in paper-based records

Employee Responsibilities

An employee is responsible for PCI compliance in the same way as any other merchant; you must protect your systems that are directly related to cardholder data whether electronic or paper based.

If you are responsible for protecting cardholder data at the point of sale and as it flows into the payment system, the best step you can take is to not store any cardholder data. If you do, it should only be for the shortest possible time in-line with the bank's recommendations, the organisation's financial regulations and with their document retention schedule.

The PCI have produced a quick reference guide to help you understand your responsibilities which you are advised to read: https://www.pcisecuritystandards.org/documents/PCISSC%20QRG%20August%202014%20-print.pdf

Importance of PCI compliance

A major priority to the card associations is assuring that cardholder information is handled in a secure manner. All merchants will be required to meet PCI compliance guidelines.

Failure to comply with the PCI security standard may result in substantial fines or permanent expulsion from card acceptance programs. Some merchants, based on transaction volume and sales acceptance channel, will be required to validate their compliance to the banks and there will be assurance checks on your systems by Internal Audit.

Computer Misuse

An exhaustive list cannot be prepared for all possible forms of misuse of computer resources. The individual circumstances of each case will need to be taken into account. However, some examples are as follows:-

- use for the purposes of fraud, theft or dishonesty
- accessing inappropriate web sites including personal email accounts, pornography, gambling/betting sites
- the storing and/or loading of software which has not been acquired through approved procedures,
- a purpose which is not work-related and is outside the Acceptable Usage Policy including personal use of social media sites within work time
- storing and processing or printing of data for a purpose which is not work-related

The use of all devicesis monitored. Where misuse is suspected, this must be reported to ICTSS, SWG who will authorise an investigation and where suspicions are valid and formal disciplinary action may be necessary HR providers must also be contacted.

Telephone misuse

The misuse of the telephone service is considered to be a disciplinary matter. All telephone usage must primarily be for Council business but occasional personal, local rate calls are permitted with line manager consent and the Acceptable Usage Policy applies.

Personal calls must not interfere with Council business, and must be kept to a minimum length of time. It is the responsibility of line managers to monitor and report a member of staff for telephone misuse.

Cloud computing and remote hosting

If your business area is considering Cloud Computing or remote hosting, please contact the ICTSS to discuss the security requirements.

Internet Misuse

All Internet usage is recorded and monitored.Where a manager suspects that the Internet facilities are being abused by a user; they should contact the ICT Solutions Manager together with the approval of a Senior Manager within their organisation. Designated staff in the ICT Department can investigate and provide evidence and audit trails of access to systems. The ICT Department will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers Act for this information.

Sharing/Sending Physical Data

Royal Mail and DX (document exchange) are the current methods for sending physical mail.

When sending documents by this method only include what is absolutely necessary i.e. remove other files and folders etc.

Anyone sending OFFICIAL – SENSITIVE data via Royal Mail or DX should do so using either the recorded or tracked mail options to ensure that it reaches its destination. Double enveloping should be considered, include a return address and **never** mark the classification on the envelope.

When faxing OFFICIAL-SENSTIVE data, information should only be sent to pre-programmed numbers. Documents sent this way should have a cover document specifying who they are intended for and the number of pages that are being faxed. Staff should contact the ICTSSService Desk for more assistance on this.

Business continuity

It is the responsibility of each organisation to make ICTSS aware of the business applications they operate when there is a reliance on central IT systems, e.g. network connectivity or backup.

The operation of business critical systems should always be notified to ICT so provision can be made for disaster recovery and business continuity at an appropriate level.

For unplanned system downtime, ICTSSexpects the appropriate level resilience for power, data loss or corruption, and business continuity.

Plans for Business Continuity are the responsibility of each organisation and will be drawn up and maintained by them. ICTSS will have in place aDisaster Recovery Plan that reflects the Business Impact Assessment on Service Provision for each organisation. ICTSS will also test their Business Continuity arrangements with the designated organisation’s Service Managers to ensure that they are robust and reliable

For planned system outages, ICTSSexpect that reasonable consultation has occurred between business owners and other parties to ensure that disruption to normal business activities, procedures and disaster recovery activities (for example backups) is minimised and acceptable.

Security Incidents

An information security incident (or breach) occurs when electronic or hard copy data or information is transferred to or received by someone who is not entitled to receive it, data is at risk of corruption or loss, or corporate hardware is lost/stolen.

All information security incidents should be reported to the ICTSS service desk and to the appropriate PSN Security Managers immediately.

Where the incident involves personal data it should also be reported as a Data Protection breach to the organisation’s Data Controller or appropriate person responsible for information security.

Training

All ICTSS users are required to attend a mandatory annual training session on information security and Data Protection. Failure to attend the training may result in the user’s access being withdrawn. The training will be organised and delivered by ICTSS who will also maintain the attendance list.

Any additional training will be provided by each organisation to add their own specific ways of working.

Monitoring and Review

This Policy will be reviewed and approved by the joint SWG and the ICTSS Joint Management and Liaison Group.Compliance with the policy will be monitored by ICTSS in respect of the areas of work covered by the ICT network and equipment.

Local security arrangements e.g. security of documents, passwords, secure areas will be the responsibility of the individual organisation's service managers

Appendix A: Removable Media business case form

Business Case for Use of Removable Media Device.

Company:	
Department / Section:	
Username:	
Type of device(s)?	
Reason for requiring device(s)?	
Frequency of use?	
Content of data held on USB device(s):	
Service Manager Name Approved:	
Date :	
SWG / IAO approval	
SWG /IAO Approved Date	
ICT Proposed Solution **(For ICT to complete)**	
ICT Call Ref Number:	
ICT Actioned Date:	
ICT Approved by:	

Appendix B: Business Case Guidance notes

Q1. Does the applicant require write access to the removable digital storage device(s) selected?

Write access allows the applicant to add data to, and remove it from the device. Careful consideration should be made as to whether the applicant should have (or need) permission to do this.

Some considerations include:

- All data should be stored on network drives and is accessible via Citrix remote working when a person is working away from the office.
- Data storage on removable media is not backed up and poses a security risk.

Q2. How does allowing the use of the device(s) assist the applicant with the delivery of the strategic objectives of the council?

You should clearly state the reasons why the applicant requires permission to store data on each of the removable media devices. “They need it to do their job” is not a valid business case.

Some examples are:

- ICT Engineers will need access to **USB hard drives**, as these are the drives they carry around that hold information for their images, and applications, these devices will only ever be connected to a user’s ICTSS-issued laptop or desktop.
- **Flash drives**, occasionally these will also have small applications on them, the devices carry less weight and hold most of the basic software an engineer will use, i.e. anti-virus, some Microsoft applications, this is in case they do not have the USB hard drives with them.
- **Digital cameras,** again these may only apply to certain staff i.e. communications officer being one.

Q3. For what duration of time does the applicant require access to the device(s)?

If the applicant requires access to the device short term please state the ‘to:’ and ‘from:’ dates. Before selecting this option consider the alternatives to allowing temporary data storage on removable devices and whether it is really necessary.

‘’Indefinitely” is for applicants who require access to the devices on a daily basis to undertake their normal work duties.

Q4. Where does this form go?

A work request must be raised on ICT servicedesk and a scanned copy of this form must be attached to the work request.

Appendix C: Cheltenham Borough Council

Building/Physical Security

The council office building is accessed by utilisation of swipe access control cards, which are authorised by line managers and issued by ICTSS to staff, Members, official visitors and contractors.

The areas to which each staff member is given access are determined by job requirement, and as such, are reviewable as required.

Members have access to the council office building to attend meetings, use the member facilities including the members' Room and to visit officers.

Certain areas in the building have restricted access due to the nature of work performed, or the vulnerability of equipment therein.

Visitors to the building are signed in at reception, and issued with a visitor's pass, which gives access to non-restricted areas of the office.

It is the responsibility of the host to ensure that the visitor is aware of the capabilities of their access card, and the procedures to follow in case of emergency, or should evacuation of the building be necessary.

It is a requirement of all staff to challenge any member of staff, members or visitors who are not displaying their identity (access) card.

It is also a requirement of all staff to prevent tailgating of others through access controlled doors throughout the building.

Any files containing personal or sensitive business information should be locked away in a secure cabinet.

When away from their desks even for short periods of time all ICT users should ensure that their computer screens are locked and any personal or sensitive business materials are not left unattended.

Service managers must undertake a risk assessment to mitigate the risk of non-authorised persons being able to see information on VDU screens i.e. through windows from outside the building.

Clear desks

All CBC employees (and members where appropriate) must clear their desks of all files and records that contain confidential, personal or sensitive data at the end of each working day.

Any files containing personal or sensitive business information should be locked away in a secure cabinet.

When away from their desks even for short periods of time all ICT users should ensure that their computer screens are locked and any personal or sensitive business materials are not left unattended.

Working from away from the office i.e. from home
When accessing or using official information at a location away from the office the user must treat the data in the same way as they would in the office e.g.. it should be kept secure, it should not be left in areas where non-authorised people can access it. ICTSS assets must also be kept secure at all times and must be locked away when not in use.

Disposal of confidential waste
Confidential waste (containing OFFICIAL - SENSITIVE or sensitive business information) is to be placed in the locked confidential waste bins within offices or shredded immediately after use.

The bins are then collected by an approved contractor who shreds the waste on site and provides the Council with a certificate of destruction.

Building and room alarms systems
Where an alarm is fitted it must be operated in-line with instructions provided by the Property Services. Any malfunction or defect must be reported to Property Services immediately.

CCTV systems
CCTV systems whether fixed or static, covert or overt they play an important role in helping the council maintain security, these systems also collect and store information which must be held securely. Any CCTV system needs to comply with the Data Protection Act, be the subject of a Privacy Impact Assessment and be supported by a published CBC CCTV Code of Practice for that system. All staff and members must comply with the arrangements of that Code; these can be found on the internet and with the appropriate Service Manager.

Appendix D: Cheltenham Borough Homes

Building/Physical Security

Redacted

Appendix E: Forest of Dean District Council

Building/Physical Security

Redacted

Appendix E: UBICO Ltd

redacted

Appendix F: Cheltenham Leisure & Culture Trust

Building / Physical Security

Leisure-at-cheltenham:

redacted

The Wilson:

Redacted

Cheltenham Town Hall / Pittville Pump Rooms:

Redacted