West Suffolk Council
Information Security Policy

Contents

1. Introduction

1.1 The effective and secure use of information is integral to the work of West Suffolk Council. The council holds and uses sensitive data and information relating to staff, customers, council finances, the local economy and emerging policies that need to be protected in order to guard against the undesirable consequences of information falling into the wrong hands.

1.2 The council has a large investment in the use of IT which is used to the benefit of all services and West Suffolk's customers. In many areas of work, the use of IT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the IT systems and data are maintained at a level which is appropriate for the council's needs.

1.3 This policy should be reviewed regularly by the council's Information Governance Working Group (IGWG) in order to account for new threats and changes in technology.

2. Policy objectives

2.1 The main objectives of this policy are to:

- protect our information and prevent data losses
- protect our IT systems and information assets from threats that compromise their effectiveness
- ensure that users are aware of and fully compliant with all relevant legislation
- create and maintain a level of awareness of the need for information security to be an integral part of daily operations, so that all users of IT systems understand the need for information security and their own responsibilities
- ensure the security of data we share both in transit through the use of encryption and through due diligence on the organisations we share with.

3. Scope

3.1 This information security policy is relevant to all services irrespective of the equipment or facility in use and applies to:

- all employees, members, consultants, agency workers, volunteers, casual workers, and agents of other organisations who directly or indirectly support the council
- all users of information throughout the council, in the field and at home or in other organisations when engaged on council business.

4. Responsibility for security

4.1 Information security is the responsibility of the council as a corporate entity and of all members of staff. A Senior Information Risk Owner (SIRO), supported by the Information Governance Working Group, has the responsibility for managing the council's information governance. The SIRO, Leadership Team (LT) and members have approved this information security policy.

4.2 This policy applies to all individuals who use any form of information, data or computer facilities that are part of the corporate IT system or contain corporate data. All users of the council's IT systems have access to e-learning materials which highlight their responsibilities and draw attention to the possible consequences of not complying with the instructions.

4.3 All senior and line managers in all services are responsible for the implementation and monitoring of the information security policy.

4.4 All third party providers of services are responsible for ensuring the security, integrity and availability of information within the service provided.

5. Legislation

5.1 The council must abide by all UK legislation affecting the information assets that we hold. All users of IT systems must comply with the following acts and guidelines and they may be held personally responsible for any breach of guidelines, current legislation (as listed below) and any future legislation that may be enacted.

- General Data Protection Regulation 2018
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom Of Information Act 2000
- Requirements and advice of the Information Commissioner on data handling and storage
- Public Services Network (PSN) connection compliance
- National Cyber Security Centre (NCSC) Cyber Essentials Plus
- Payment Card Industry (PCI) guidelines governing the taking of electronic payments.

Information about the above acts can be found on the government website Legislation.gov.uk and guidelines on information security can be found at Information Commissioner's Office or from the council's Data Protection Officer who can be emailed at data.protection@westsuffolk.gov.uk. The key points of relevance to West Suffolk are covered in the e-learning materials available to all IT users.

6. Standards and procedures

6.1 Physical access to information resources

6.1.1 Precautions must be taken to ensure that access to desktop and laptop PCs, tablets and smart phones is restricted at all times to authorised personnel.

6.1.2 Equipment should be sited to reduce the risk of damage, interference and unauthorised access.

6.1.3 When equipment is left unattended for an extended time, such as overnight, it must be powered off. Mobile equipment, such as laptops, tablets and smart phones, must be locked away in offices and never left on view in unattended vehicles.

6.1.4 All appropriate computer equipment will be identity tagged and be recorded on the central West Suffolk IT inventories. It is the responsibility of line managers to notify the West Suffolk IT Helpdesk of any movements or changes.

6.1.5 Where computer equipment is to be used away from council buildings, for example when mobile working or using at home:

- all of the provisions of this policy document apply
- the council's agile working policies must be adhered to
- any individual using a device at home or in the field is responsible for ensuring the safety and security of both the equipment and any data contained thereon
- equipment must only be used outside the UK with the agreement of IT. When using any equipment outside the UK, confidential data should not be handled.

6.1.6 No equipment purchased, leased or hired by a user department may be connected to the council's IT systems (including, but not limited to, on-premise network and cloud systems) or attached to any equipment connected to IT systems without authorisation from the IT Infrastructure and Cyber Security Manager. IT should be asked to review the specification of any technology that requires additional devices or software to be connected or run on the council's IT systems before it is ordered. The restriction also applies to any equipment not owned, leased or hired by the council. This includes, but is not limited to, USB memory sticks, tablets, smart phones and other devices. Where permitted, all such equipment must be supplied or confirmed as suitable by the West Suffolk IT Team.

Access to the council's Microsoft 365 systems (including calendar and email) are available on personal iPhone/iPad and Android phone and tablet users via the council's secure Mobile Application Management

system where business need dictates and will be operated in accordance with the council's separate Bring Your Own Device guidance.

6.1.7 The following precautions should be taken to ensure that only authorised personnel have admission to office areas where there is access to IT systems or sensitive data. Such precautions include:

- identity cards should be carried at all times and presented if challenged
- visitor procedures for the building you are working in should be followed – for example, West Suffolk House visitor procedures
- staff should challenge anyone within council buildings with no visible identity badge if they suspect that they may be unauthorised visitors
- where Principles of Occupation exist for offices, staff should adhere to any relevant clear desk policies to ensure sensitive data is protected when desks are left unattended.

6.2 System access

6.2.1 Requests to provide access to IT systems should be made initially through your line manager or service manager.

6.2.2 Passwords will be set to prevent unauthorised access to data held on IT devices. The use of initial logon passwords is especially important in the case of laptop or notebook PCs, tablets, smart phones and other devices that are portable and therefore less physically secure. Users must not disclose their personal password to anyone. However, in some exceptional cases, a shared PC may have a password known by several users within an office to enable access – for example, front of house logons and training room logons. In these instances, the shared logon account is restricted for use only on certain PCs and permissions are severely limited in terms of wider access. Where these shared logons exist, line managers are responsible for ensuring that shared passwords are used solely by authorised personnel and that passwords are changed when staff leave their teams.

6.2.3 Unique usernames will be allocated by the system administrators. Wherever possible, these will be consistent across systems. Access levels will be determined and implemented by systems administrators for each system area. Likewise, access to any shared IT resources – for example, printers – can be given by West Suffolk IT.

6.2.4 If staff know they are leaving sight of their desk for any period, they should lock their workstation, which not only blocks any sensitive information from view, but also prevents access without the relevant password to unlock the device. If the screen is not locked by the user, an automatic screen saver is set to lock the screen after 10 minutes of inactivity on any West Suffolk PC.

6.2.5 A corporate 'null' screensaver will be provided giving immediate complete screen confidentiality and should be used in conjunction with a password. This will automatically be set after a maximum duration of 10 minutes. Unauthorised screensavers are not permitted as they can cause unacceptable overloading of IT devices and servers.

6.2.6 Passwords must be used to protect all systems and should not be written down or disclosed to others not properly authorised to use them. All users of IT systems will be held liable for any misuse of a computer resulting from use of their personal password or username. Passwords must be changed to a previously unused password at least every 365 days in line with the policy as set out in Appendix A. Passwords will automatically expire if not changed within this frequency which prevents access to the council's IT systems.

6.2.7 System administrators must be notified immediately by the leaver's line manager of all leavers to enable the timely removal of all access rights.

6.2.8 All access across the Internet to the council's IT systems will be authenticated via Multi Factor Authentication (MFA). At present, this is provided via Corporate MFA App, TPM chip in corporate devices or Internet Protocol (IP) address restrictions.

6.3 Information and data

6.3.1 Information held on the council's IT systems or subsequent output, for example printed letters or tabulations, is the property of the council and is governed by the provisions of the Data Protection Act. Any purpose for which personal information is held must be registered under the Act by the council's Data Protection Officer who can be contacted at data.protection@westsuffolk.gov.uk

6.3.2 Information and data held or transmitted, for example through email, is subject to the West Suffolk and/or National Protective Marking Scheme as explained in Appendix E. Data marked confidential must not be sent outside the council unless encrypted.

6.3.3 Information held should only be released to authorised persons or where an information sharing agreement is in place. IT facilities supplied must only be used for authorised purposes. IT facilities should normally only be used for work-related purposes. However, occasional and reasonable personal use is permitted. Such activity must not prejudice or interfere in any way with the council's IT facilities or its business activities. Any such use should be carried out in staff's own time. Excessive use or any use for personal commercial gain is not permitted. No additional software will be loaded to facilitate personal use.

6.3.4 Any personal or sensitive data displayed upon unattended equipment must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so. This is applicable to information displayed on monitors, printed output and computer produced media such as microfiche.

6.3.5 All portable devices supplied by West Suffolk IT or owned by West Suffolk Council must be encrypted to the latest National Cyber Security Centre (NCSC) standards using 256bit AES encryption. However, users should still avoid storing confidential data on local devices, such as C:\ drives, mobile devices such as laptops, smart phones or USB memory sticks, where possible. Writing to unencrypted removable media is blocked by default on all council devices. Further guidance is provided in Appendix B.

6.3.6 No information of a personal or sensitive nature shall be sent outside the council's IT systems unless authorised and encrypted or, where appropriate, sent using one of our secure mail methods. For information on how to do this please review our latest guidance: West Suffolk Council – Secure emails

6.3.7 Documents containing confidential or sensitive information should never be sent to a non-council email address. If staff are not home-enabled, they should speak to the West Suffolk IT Helpdesk about how such documents can be safely transmitted. Automatic or 'blanket' forwards from any West Suffolk managed email domains such as @westsuffolk.gov.uk, @angliarevenues.gov.uk addresses to non-council addresses will never be configured by IT on the mail system and must not be setup by users via the Outlook rules wizard. It is important that customers and users of the council's IT environment know that when they send to these addresses the information does not leave the council's IT systems in a non-discretionary way and is therefore secure.

6.3.8 Care should be taken when using social media such as Facebook and X as information entered on this type of site is readily available in the public domain. Further information and guidance can be found in the council's separate Social Media Policy document.

6.3.9 No confidential information should be provided in response to online surveys (for example sales surveys) sent to the council by other agencies as the software used may be hosted outside the EU and therefore not be bound by the same data protection rules as the UK.

6.3.10 All data held on the council's IT systems or on any device used by staff and agents should only be held for a period appropriate to its relevance and erased or destroyed in line with the council's Data Retention Policy.

6.3.11 Security of data and data protection rules apply equally to paper based documents, therefore sensitive documents and those containing personal information:

- should not be left unattended and should be locked away at the end of the day
- should be disposed of in the bins marked as specifically allocated for confidential items
- if being taken out of the office or worked on at home, should be stored in a lockable cabinet or case at home.

In addition, all workstations should be left clear at the end of the day.

6.3.12 All computer output no longer required by the council should be disposed of with due regard to its sensitivity. Confidential output should be disposed of in secure bins located around all council offices. All forms of electronic storage media, including but not limited to Microfiche, CD or DVD-ROM, memory sticks and other magnetic or optical media, should be disposed of appropriately or be securely erased. Data on inbuilt hard disks will be erased by the West Suffolk IT Team before any re-use or disposal as defined in section 6.8.

6.3.13 Any queries relating to the provisions of the Data Protection Act and how it affects your operations should be directed to the council's Data Protection Officer at data.protection@westsuffolk.gov.uk.

6.3.14 All users are responsible for setting file or folder permissions to ensure data is only accessible to the relevant authorised staff. Training and advice on this is coordinated by the West Suffolk IT Team.

6.4 Virus protection (including malware and ransomware)

6.4.1 All PCs (including laptops and tablets) are protected by virus protection software which is upgraded and monitored regularly by the West Suffolk IT Team. Any detected or suspected malicious activity must be reported to the West Suffolk IT Helpdesk immediately.

6.4.2 All removable media, CD-ROMs, USB memory sticks or other USB devices will be virus checked automatically prior to use in any of the council's computers. This is especially relevant where disks have been received from an external source.

6.4.3 Removable media, CD-ROMS, USB memory sticks or other USB devices must not be inserted into PCs until after the logon or initial password has been entered and the computer has reached:

- the point where you log into the council's IT systems
- the Windows screen on stand-alone PCs.

6.5 Software copyright

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

6.5.2 The loading of proprietary software programs for which a licence is required but not held is prohibited and this is also an offence which could lead to a fine or imprisonment. All software installation media and licences must be held by the West Suffolk IT Team.

6.5.3 Personal software (for example games) must not be installed or run on the council's IT systems under any circumstances. If the software is deemed to be of use to the council, then it should be duly acquired under licence. All software must be approved by senior IT management (grade 8 or above) before purchase to ensure compatibility with West Suffolk IT systems.

6.5.4 Spot checks may be conducted by the West Suffolk IT Team and/or auditors to ensure software licensing compliance. Authorised personnel from IT and Audit have rights of access to all systems, the power to seek explanations from members of staff concerned and the right to remove any unauthorised software found to have been installed.

6.6 Computer misuse

6.6.1 All employees should be aware of the access rights they need and are assigned to conduct their duties and must not attempt to experiment or attempt to access the council's IT systems or data for which they have no approval or need to conduct their duties.

6.6.2 All IT users are required to comply with the email and Internet usage policy issued on behalf of the council.

6.7 Contingency planning

6.7.1 Security copies (backups) should be taken at regular intervals dependent upon the importance and quantity of the data concerned. In the case of systems and data residing on the council's IT infrastructure, the West Suffolk IT Team will take them on behalf of users at appropriate intervals. Where services are using Software as a Service (SaaS) systems, they should ensure recovery time objectives (RTO) and recovery point objectives (RPO) that the supplier offers are appropriate for their service.

6.7.2 In the case of corporate personal computers, the prime copy of all data files must be held on the appropriate network drive. Advice on changing the default(s) from the local C drive on PCs to space on the appropriate server is available from the West Suffolk IT Helpdesk. However, it is the responsibility of individual members of staff to place their data files in the correct location.

6.7.3 Arrangements must be in place and procedures specified by the relevant service manager, in conjunction with the West Suffolk IT Infrastructure & Cyber Security Manager, to ensure critical systems/operations are able to continue in the event of complete computing failure. These will primarily be provided through business continuity plans coordinated by the council's Emergency Planning Team.

6.7.4 Security copies should be stored away from the system to which they are related in a restricted access fireproof location. Security copies should be regularly tested to ensure that they enable the system or relevant file to be reloaded in an emergency.

6.7.5 Security copies should be clearly marked as to what they are and when they were taken. Depending on the importance of the system concerned, they should provide for system recovery at various different points in time over a period of several weeks.

6.8 Acquisition and disposal of IT products

6.8.1 All acquisitions should be in accordance with the provisions of the council's IT frameworks and their financial regulations. Any queries should be directed to the West Suffolk IT helpdesk, email IT.help@westsuffolk.gov.uk

6.8.2 The disposal of IT equipment must be coordinated through the West Suffolk IT Helpdesk who will arrange for the permanent removal of all data and software licensed to the council unless the recipient is taking over the licence and is authorised to use it.

6.8.3 The disposal or permanent handover of equipment, media or output containing personal or sensitive data must be arranged in a way that ensures confidentiality.

6.8.4 Wherever possible, consideration is given by West Suffolk IT to the reallocation of equipment within the council.

6.9 Suspected security incidents, loss or theft of equipment and data

6.9.1 All staff have a duty to report immediately any suspected security incidents. Such information shall be regarded as confidential by all employees involved, and should be reported to the Audit Section, West Suffolk IT Help Desk, Data Protection Officer, Insurance Officer and the council's SIRO.

6.9.2 Loss or theft of any council-owned device or personal phone with BYOD access must be reported to the West Suffolk IT Help Desk by phone at the earliest possible opportunity. The IT Helpdesk is available 8.15am to 5.30pm, Monday to Friday. Outside these hours, IT can be contacted via the emergency out of hours service 01284 763252. Any device that has remote access to council systems will immediately have its remote access disabled.

6.9.3 When such an incident is reported, the West Suffolk IT Infrastructure & Cyber Security Manager will conduct an immediate investigation with the appropriate director to establish whether any data lost is of a personal or sensitive nature and to assess any consequential business risk it poses. The Audit Team will also conduct an investigation to establish whether there has been a breach of this policy or any other relevant rules or statute and whether appropriate action must be taken.

6.9.4 Where a data breach is identified to have compromised an individual(s), those individuals must be notified by HR as soon as possible and steps

taken to minimise the risk of potential fraud or loss to the individuals affected.

6.9.5 Any data breach shall also be investigated and, if necessary, the office of the Information Commissioner informed by the council's Data Protection Officer. A full report of the incident with a list of actions taken, together with a plan of steps required to be taken to reduce risk of recurrence.

6.9.6 All breaches of information security (whether stolen or by accident) must be reported to the Data Protection Officer at data.protection@westsuffolk.gov.uk. The penalties for a data breach can be severe, with councils risking six-figure fines for data losses.

6.9.7 A checklist of the actions in section 6.9 can be found in Appendix C.

7. Violations

Violations of this information security policy may include, but are not limited to, any action that:

- exposes the council, its members, staff or customers to actual or potential monetary loss, or loss of reputation, through the compromise of information security
- involves the disclosure of confidential information or the unauthorised use of data
- involves the use of data for illicit purposes, which may include violation of any law, regulation, council's policy, or any reporting requirement of any law enforcement or government body
- falls within the terms of computer misuse in section 6.6 above.

8. Disciplinary process

West Suffolk takes information security seriously and any breach of this policy could lead to disciplinary or legal action being taken against anyone who commits a breach, in accordance with the Disciplinary Policy and the Disciplinary Rules. Violations such as the use of unauthorised software, the use of data for illicit purposes or the copying of software which breaches copyright agreements will be investigated in accordance with the Disciplinary Policy and serious or wilful actions taken in breach of this policy are likely to be treated as gross misconduct and appropriate action taken, which can include summary dismissal.

Appendix A: Policy use and control of passwords

Wherever possible, the council follows the latest guidance on password policy issued by the National Security Centre (NCSC). The following password rules should therefore be adhered to on all systems in use at West Suffolk Council.

1. Passwords must be a minimum of 15 characters.

2. Passwords must contain characters from four of the following four categories:

    - English uppercase characters (A to Z)
    - English lowercase characters (a to z)
    - base 10 digits (0 to 9)
    - non-alphabetic characters (for example, !, $, #, %).

3. Your password must not contain your username or parts of your full name.

4. Your password must not contain three consecutive identical characters.

5. Names that are likely to be easily associated with the user – spouses', children's or pets' names for example – should be avoided. Passwords must not include the word 'password' itself. The council now employs the use of password 'denylists' to prevent easily guessable dictionary words being used for its main logons. The council recommends the use of three random words within passwords to meet these requirements while making passwords easy to set and remember.

6. You will not be allowed to re-use any of your previous 24 passwords.

7. Personal passwords must never be written down either in hard copy or in plain text electronic versions. Use of a password manager is permitted – staff should familiarise themselves with the current NCSC online guidance on the use of password managers. Shared passwords must never be written down and left in insecure locations. Where shared passwords need to be written down, they should be stored in a secure location such as a fire safe.

8. Personal and system passwords must be changed at least every 365 days. The system will prompt you to change your password every 365 days. Where possible, systems should be set to force a change of password at regular intervals.

9. Managers must ensure that passwords known to staff who leave the council's employment are changed immediately on their departure.

10. The council regularly monitors passwords exposed in public data breaches. You may be requested to change your password at any time if we believe it has been compromised.

Notes

For the majority of systems, the ability to change passwords lies directly with the end user; this allows you to change your own password. Where this is not the case, this function is carried out by the system controller who will ensure that passwords are changed for you.

Some systems are set to force users to change passwords after a set period of time; the time period can be varied with the assistance of West Suffolk IT staff.

All managers are responsible for ensuring compliance with this policy.

Appendix B: Advice on storage of computer files

Where should you NOT store files?

On the local hard disc on a desktop PC (Drive C). This includes:

- 'Documents' (unless you have set it to be redirected to a network drive)
- the 'Windows Desktop'.

Although normally encrypted, these locations are not as secure as network drives and SharePoint, if the IT device is lost or stolen, data could be misused. These locations are not routinely backed up centrally. Therefore, if the hard drive on your device was to fail, or you delete a file, we will not be able to recover them from the central backups.

Please note: portable devices are encrypted to NCSC standards using AES256bit encryption. However, storing files locally should still be avoided where possible.

If you want to access files from your desktop, create a shortcut to the file on the network drive or SharePoint. To create a shortcut, right click on the file, select SEND TO, then left click on Desktop (Create Shortcut).

If necessary, it is possible to create copies of files or folders. To do this, laptop users can set up offline synchronisation. You can select folder contents to be available when you are not connected to the network. When you are connected to the main network and log on or off, these files will synchronise in both directions. Under no circumstances must this be used for personal or confidential data. If you are in any doubt about what is classed as confidential data, seek guidance from your line manager or the council's Data Protection Officer at data.protection@westsuffolk.gov.uk

What are the storage locations?

Default storage locations are either traditional network drives or SharePoint sites, and are where users can conceivably store files but the decision as to which location is appropriate must be taken according to the nature, sensitivity and need to enable access to other users – not all locations are appropriate for all types of data**.** Drive letters may vary for different organisations.

- **K Drive** – also known as the public area. If you wish to share work among staff from several services, you may create a folder here and place work in it. Remember to set the folder permissions to allow access only to those staff you wish to have access; by default, **everyone** can access data.

- **S Drive** – also known as the service drive (for example, Resources and Performance, Operations, HR Governance and Regulatory). This will allow you, depending on the folder permissions, to access the section folders. This is mainly there for staff who work for several services to easily move about between the section folders.

- **T Drive or Team SharePoint site –** also known as the team area. This is where the majority of your work should be stored and, as such, you should

set the Microsoft applications to default to this location. If you're unclear about how to do this, contact the West Suffolk IT Helpdesk on 7677 or IT.help@westsuffolk.gov.uk

- **One Drive –** also known as the user's personal drive. This is where you should keep personal files (CVs, personal development reviews and so on). Only someone logged on as yourself will be able to access this area. You should not store any files here that might require access by other members of staff. These must be stored within the T drive or your Team SharePoint site.

Some services and teams will have other mapped drives for software specific to their section or user.

Appendix C: Checklist of actions for suspected security breach

Action	Responsible officer	Completed
Report any suspected security incidents immediately. Such information shall be regarded as confidential by all employees involved and should be reported to West Suffolk IT Helpdesk who will inform the following as appropriate: • Audit Team • Data Protection Officer • Insurance Officer • your director or line manager • Monitoring Officer (elected members) • Head of Service (Human Resources and Organisational Development)	Staff member	
National Cyber Security Centre (NCSC) - www.ncsc.gov.uk	West Suffolk IT Infrastructure and Cyber Security Manager	
If any mobile device has been lost or stolen which allows remote access to the council's IT systems, immediately ensure that the device account is disabled and no replacement issued before next step (below) is completed.	West Suffolk IT Helpdesk between 8.15am and 5.30pm, Monday to Friday West Suffolk Emergency Out of Hours Service 01284 763252	
Conduct an immediate investigation with the appropriate director to establish whether any data lost is of a personal or sensitive nature and any consequential business risk it poses to the council.	West Suffolk IT Infrastructure and Cyber Security Manager	
Conduct an investigation to establish whether there has been a breach of this policy or any other relevant rules or statute and whether appropriate action must be taken.	Audit Team	

Where it has been established that a data breach has compromised an individual or set of individuals, those individuals must be notified as soon as possible and steps taken to minimise the risk of potential fraud or loss to the individuals affected.	If staff, then the Head of Service (Human Resources and Organisational Development) If members of the public, then relevant director	
Investigate any data breach and if necessary inform the Office of the Information Commissioner with a full report of the incident and a list of actions taken.	Data Protection Officer	
Submit a proposal of future preventative steps required to be taken to reduce risk of recurrence to Leadership Team (LT).	West Suffolk IT Infrastructure and Cyber Security Manager	

Appendix D – IT security dos and don’ts

Do:

- keep passwords to yourself
- change passwords regularly
- keep your files on network drives or SharePoint (for example, K, S, T and U)
- lock your IT device when leaving your desk
- lock your mobile IT devices away in a secure location if you leave them in an office overnight
- lock your laptop out of sight in your boot (if you have to leave it in your car at all)
- log off then switch off your PC at the end of each day before you leave
- report suspected data loss or theft immediately to your line manager
- when travelling away from the office, make sure your laptop is secure and not left unattended.

Don’t:

- tell anyone your password
- write your personal password down
- respond to suspicious emails (spam)
- store files on ‘desktop’, ‘C:’ drive or ‘Documents’
- send personal or sensitive data via email without encryption
- leave your mobile IT devices on your desk overnight
- leave your mobile IT device on view in unattended vehicles
- leave your mobile IT device on view in public places
- use USB memory sticks or other easy to lose devices to store sensitive data.

Appendix E – Protective marking schemes

1. West Suffolk Protective Marking Scheme

The Information Governance Working Group (IGWG) has agreed the use of a local marking scheme across the council as follows:

- **Exempt or confidential** – data that contains sensitive information relating to staff, customers, policy development, financial information
- **Unmarked** – all other non-confidential data.

2. Government Protective Marking Scheme

Users who exchange information with government departments such as the DWP should familiarise themselves with the National Protective Marking Scheme. Staff should review the current guidance and standards published on GOV.UK – Government security classifications