West Lindsey DISTRICT COUNCIL

Information Security Policy

Acceptable Use Policy

Version Number	Draft 0.1
Approved by	
Date approved	
Review Date	
Authorised by	
Contact Officer	Data Protection Officer

Revision History

Revision Date	Version	Description of Revision

Contents

1 Introduction

1.1 Information plays an essential role in the conduct of the business of West Lindsey District Council (WLDC, “the council”)

1.2 The information technology and communications facilities must be used sensibly, professionally, lawfully, consistently with the duties of the role, with respect for colleagues and in accordance with this policy and with the council’s rules and procedures. The Information Technology infrastructure is either wholly owned by or operated on behalf of WLDC and consequently any information contained therein is owned by the council.

1.3 Acceptable use means that access to information is legitimate, it is used only for the intended purpose(s), the required standards of practice are in place to protect the confidentiality, integrity and availability of information, and the use complies with relevant legislation and regulation.

1.4 All references in this document to WLDC or “the council” shall be deemed to refer to West Lindsey District Council and any other organisation which the council wholly or partly controls.

1.5 This policy forms part of WLDC's compliance with the Payment Card Industry - Data Security Standard (PCI-DSS) and the council’s commitment to comply with the principles of ISO27001:2013 "Information Security Management System" and Cyber Essential Plus.

1.6 This policy will be published on the council’s intranet (Minerva) and any amendments or revisions will be notified to all staff.

2 Policy Statements

2.1 It is the responsibility of all users to know this policy and to conduct their activities accordingly. Breach by any user could result in disciplinary action or other appropriate action being taken.

2.2 Council information facilities are provided for business purposes only, with limited personal use permitted as defined elsewhere in this document.

2.3 Use of information facilities must be authorised by line managers.

2.4 Any use of council facilities for unauthorised purposes may be regarded as improper use of facilities. Council IT systems must display an appropriate warning notice to this effect when users log on.

2.5 Users should be aware that any data they create on council systems (including anything pertaining to themselves) is deemed to be the property of the council. Users are responsible for exercising good judgment regarding the reasonableness of personal use and to be compliant with the Officer Code of Conduct.

2.6 For security and network maintenance purposes, users specifically authorised for the task may monitor equipment, systems and network traffic at any time.

2.7 The council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.8 The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact your line manager.

2.9 This policy is supported by a number of other policies and standards which should be read in conjunction with it:

1. Data Protection Policy
2. Information Security Policy
3. Information Security Incident Management Policy
4. Information Classification and Handling Policy (TBD)
5. Home Working Security Policy (TBD)
6. Payment Card Industry-Data Security Standard (PCI-DSS) Policy
7. Social Media Policy
8. Telephone Monitoring Policy
9. Telephone Recording Policy
10. Customer Standards Handbook
11. Officer Code of Conduct

3 Objectives, aim and scope

3.1 The objective of this policy is to protect the information assets (e.g. any computer system, information and data) owned and used by WLDC, from all threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements, specifically:

- Computer Misuse Act 1990
- Copyright, Design & Patents Act 1988
- General Data Protection Regulation (GDPR)

- Data Protection Act 2018 (DPA)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- The Human Rights Act 1998.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (amended in 2004, 2011, 2015, and 2016)
- The Electronic Communications Act 2000.
- Obscene Publications Act 1959
- Protection from Harassment Act 1997
- Equality Act 2010
- Regulations of Investigatory Powers Act 2000
- Telecommunications Act 1984
- The Children Act 1978
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 or successor legislation
- Payment Card Industry (PCI) Data Security Standard (DSS)
- The Re-use of Public Sector Information Regulations 2015

3.2 It is a criminal offence under the Computer Misuse Act 1990 to deliberately attempt to access a system to which no authority has been given.

3.3 It is a criminal offence under Section 170 of the DPA to knowingly or recklessly obtain, retain, disclose, or procure the disclosure of personal data without the consent of the data controller (i.e. the council).

3.4 It is a criminal offence under Section 171 of the DPA for a person to knowingly or recklessly re-identify information which was previously de-identified personal data without the consent of the data controller.

3.5 It is a criminal offence under Section 173 of the DPA for the controller or an officer or other person subject to the direction of the controller to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

3.6 The aim of the policy is to ensure that staff are given the relevant support so they are aware of what is acceptable use of any computer system owned or operated by the council and can therefore apply procedures accordingly.

3.7 This policy applies to all employees, third parties, contractors and temporary staff of WLDC and compliance with its principles is mandatory for computer users accessing any computer system owned and/or operated by the council or on its behalf by a third party. Its application extends to the use of all such equipment wherever situated.

4 Responsibilities

4.1 Ultimate responsibility for ensuring compliance with this policy rests with the council's Management Team (MT).

4.2 The Senior Information Risk Owner (SIRO) is responsible for managing, implementing and effectively cascading the policy.

4.3 The Finance and Business Support Manager is responsible for PCI-DSS compliance.

4.4 The ICT Manager is responsible for implementing a secure IT infrastructure with effective controls to facilitate compliance with this policy.

4.5 Employees, third parties, contractors and temporary staff are responsible for ensuring that they comply with the requirements detailed in this policy.

4.6 Any actual or suspected breach of this policy within, or affecting, the council's systems will be thoroughly investigated. Disciplinary action may be taken against council employees in line with the relevant disciplinary procedures. Any action taken internally does not preclude prosecution through a court of law. In the event of an issue arising from a misinterpretation of this policy, it must be resolved by reference to the SIRO.

5 Confidentiality and the use of personal data

5.1 Employees, third parties, contractors and temporary staff, as part of their employment or relationship with the council, could be given access to information that is of a personal, confidential and/or proprietary nature. This might be, for example: personal information related to staff, members and citizens, such as names, e-mail addresses, salaries, employment information, health data, financial information, criminal conviction data, commercial-in-confidence or proprietary information, etc.

5.2 All employees, third parties, contractors and temporary staff therefore agree:

- To hold all personal or confidential information in trust and strict confidence, use it only for the purposes for which it was collected, and not

disclose it to any third party unless properly authorised to do so by the council.

- To keep secure any personal or confidential information in their possession.
- Not to remove any personal or confidential information from council premises without proper authorisation. Any information which is approved to be removed from council premises must be adequately protected from unauthorised use, reproduction or disclosure.
- To maintain the absolute confidentiality of personal, confidential and proprietary information in recognition of the privacy and proprietary rights of others at all times, and in both professional and social situations.
- To comply with all privacy laws and regulations, which apply to the collection, use and disclosure of personal information.

5.3 Employees, third parties, contractors and temporary staff must understand that a breach of confidentiality or misuse of information could result in disciplinary action up to and including termination of employment.

5.4 Users must only use personal data in accordance with the agreed and published purposes for the collection of data. Using personal data in any manner requires a clear legal basis or consent from the data subject. Merging personal data with other sources, for example, is not permitted unless a legal basis or consent is present, and the use of the data correctly authorised. Personal data may not be held on any WLDC computer without the authorisation of the SIRO.

6 Copyright compliance

6.1 Copyright law, which governs the use of intellectual property, including software, is very straightforward - it is illegal to use copyrighted material unless expressly permitted by the copyright holder.

6.2 Users must not:

- Transmit copyright software from their PC or allow any other person to access it from their PC unless the controls/licence so permits

- Knowingly download or transmit any protected information/material (including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources and copyrighted music) that was written by another person or organisation without getting permission

6.3 If caught using illegally using copyrighted material, it is not only the council that may face legal proceedings, but individual employees, third parties, contractors and temporary staff may also be charged with criminal and/or civil liabilities. Should such a prosecution be brought, the potential harm to the good name of the council will be immense.

6.4 Legitimate copies of software will be provided to all users who need it, subject to the necessary authorisation having been obtained.

6.5 Employees, third parties, contractors and temporary staff are NOT allowed to make unauthorised copies of any software under any circumstances.

6.6 The council will not tolerate the use of unauthorised copies of software. Any employees, third parties, contractors and temporary staff illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment, in addition to the council's disciplinary procedure.

6.7 WLDC developed software may be given to any non-WLDC employees, third parties, contractors and temporary staff, but only if specific authorisation is given.

6.8 Any misuse of software within WLDC must be promptly reported using the Information security incident reporting procedure.

6.9 All software to be purchased must be on the approved software list. The ICT Manager will ensure that a central list is created and maintained accordingly.

6.10 ICT will be responsible for completing the registration of all software with the supplier, installing upgrades and maintaining version control on all software throughout the council. ICT will ensure that all applicable licensing conditions in respect of all software loaded by them are fully met.

6.11 The loading of games, screen savers or unauthorised software on any computer system owned or operated by the council is strictly prohibited.

6.12 WLDC software must not be loaded on to any computer system not owned or operated by the council unless specifically authorised by the SIRO.

6.13 The use of Freeware and Shareware software is only permitted for appropriate business purposes if the software is shown in the approved software list.

6.14 All WLDC computers are regularly audited, as part of the conditions of complying with, but not necessarily being certified to, the standards of the Federation against Software Theft (FAST).

6.15 All software, information and programmes developed for and/or on behalf of the council by employees, third parties, contractors and temporary staff, during the course of their employment remain the property of the council. Duplication or sale of such software without the prior consent of the council will be an infringement of the council's copyright and will be dealt with as a disciplinary matter.

6.16 Software developed for or on behalf of the council must comply with this policy.

7 General security

7.1 The council has procedures in place to deal with the threat of invasive viruses, the risk of theft of hardware and software, the unauthorised access of data and the maintenance of systems security.

7.2 Employees, third parties, contractors and temporary staff must not disclose information relating to WLDC IT facilities to anyone outside of the council without the SIRO and IT Manager's express permission. Any telephone canvassing for information must be passed directly to the SIRO or IT Manager.

7.3 Computers logged onto the network must be locked (press the "windows" key and the letter "L" key at the same time) or logged off the network if left unattended. A password protected screen saver must activate after 1 minute of inactivity on the PC. If this does not occur, then you should report the matter to your service desk.

7.4 The council regularly monitors all systems and all unauthorised attempts at accessing systems are investigated.

7.5 Data must be saved on an approved network storage location. The only circumstance where data may be saved to the hard disk or authorised removal media is when a laptop is being taken to a site where the council's network is not accessible. In this event, a copy of all the data must be left on the network as a backup.

7.6 Payment card holder data must not be stored outside the council's cardholder data environment. Refer to the PCI-DSS Policy for more information about the security standards and regulations relating to taking card payments.

7.7 The responsibility for all data on the network servers lies with the ICT Manager, who will ensure that regular backups are performed, tracked and stored off site and that they are securely destroyed when the data retention periods are exceeded.

7.8 Only authorised third parties are permitted to move any WLDC IT equipment, whether within an office or to another site, unless specifically approved by the ICT Manager.

7.9 No peripheral device of any kind (e.g. digital cameras, PDAs, USB pen drives, etc.) may be installed or configured on any WLDC computer, unless specifically approved by the ICT Manager.

7.10 Disposal of WLDC IT equipment will be arranged by the ICT Manager with due regard to legal (software compliance) and environmental issues, ensuring that the appropriate hardware and software registers are updated. Payment cardholder data will be securely destroyed in compliance with the PCI-DSS.

8 Password policy

8.1 All computer users are given a BitLocker key, username and password; these are unique and must not be shared with any other employees, third parties, contractors and temporary staff.

8.2 Passwords must not be written down.

8.3 Passwords must be hard to guess and must contain at least ten characters. The minimum password requirement is that it has to include three of the four following types of character:

- Number
- Lower case letter
- Upper case letter
- Special character such as [! # £ $].

8.4 Passwords must be changed at regular intervals; systems will be configured to automatically force password changes every 365 days and to prevent re-use of the user's previous 24 passwords.

8.5 Password changes will be automatically prompted for when a password expires. To complete a password change the current password will need to be entered and a new password entered twice. The password will be validated to ensure it matches the guidelines in Appendix 1. Any typing mismatches between the new password and the retyped new password will result in the password change process being repeated.

8.6 An account will be locked after three failed password attempts.

8.7 For further password guidance please refer to Appendix 1.

9 Email acceptable usage

9.1 The council provides email to assist employees, third parties, contractors and temporary staff in the performance of their jobs and its use should be limited to official WLDC business.

9.2 However, incidental and occasional personal use of email is permitted by the council, with the understanding that personal messages will be treated in the same way as business messages.

9.3 Personal use of the email system must never impact upon normal traffic flow of business related email. WLDC reserves the right to purge identifiable personal email to preserve the integrity of the email system. As a general guide, it would not be reasonable to see more than two or three personal emails a day each of no more than one or two short paragraphs in length.

9.4 Under no circumstances should users email material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy, or which could reasonably be expected to be considered inappropriate. Any user who is not clear about whether material is appropriate should consult their team manager before starting any associated activity or process.

9.5 ICT facilities provided by the Council for email should not be used for:

- sending unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations;
- the unauthorised sending to a third party of OFFICIAL-SENSITIVE, confidential or material containing person identifiable information (PII) material concerning the activities of the Council;
- sending material that infringes the copyright of another person, including intellectual property rights;

- activities that unreasonably waste staff effort or use network resources, or activities that unreasonably serve to deny the service to other users;
- activities that corrupt or destroy other users' data;
- activities that disrupt the work of other users;
- the creation or sending of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- the creation or sending of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- the creation or sending of material that is abusive or threatening to others, or serves to harass or bully others;
- the creation or sending of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs;
- the creation or sending of defamatory material;
- the creation or sending of material that includes false claims of a deceptive nature;
- so-called 'flaming' – i.e. the use of impolite terms or language, including offensive or condescending terms;
- activities that violate the privacy of other users;
- unfairly criticising individuals, including copy distribution to other individuals;
- publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author;
- the creation or sending of anonymous messages – i.e. without clear identification of the sender; or
- the creation or sending of material which brings the Council into disrepute.

9.6 All email messages must be sent or received using WLDC's email system, the use of any other email systems including internet email (i.e. Yahoo mail, Gmail etc.) is strictly prohibited, unless specifically approved by the SIRO.

9.7 Payment card holder data must not be transmitted using messaging technologies. If a messaging technology communication is received containing cardholder data it must be logged as a security incident, deleted and removed from the deleted items folder.

9.8 All emails sent or received will be logged and when considered appropriate and properly authorised by a director and/or the Human Resources Manager, may be monitored, opened and read by appropriately authorised WLDC staff.

9.9 E-mails concerning illegal activities must not be sent or forwarded unless they relate to the legitimate business of the council. The SIRO must be notified immediately should any such e-mails be received. These emails must not be forwarded to anyone unless required by the SIRO.

9.10 The system may not be used for personal financial gain, other than for selling your own personal possessions on either a WLDC intranet site or internet sites such as eBay, but with a non-council email address.

9.11 The forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Also virus warnings come under the same exclusion; the majority of these are false, to check the truth of these messages consult with ICT, but do not under any circumstances forward these messages to anyone inside or outside of the council.

9.12 All email messages that are sent externally from the council will be passed over networks owned by other people; this is not a secure form of communication. If the content of the message could cause embarrassment or problems for the council or financial loss should the contents become known, a more secure method should be used.

9.13 The user logged in at a computer will be considered to be the author of any messages sent from that computer. Remember to log-out or lock computers if left unattended (press the “windows” key and the letter “L” key at the same time). Under no circumstances should an e-mail be sent from a PC that is logged in to the network by another person. Email addresses should not be disclosed unnecessarily.

9.14 Disclosing email addresses when filling in surveys or other questionnaires will increase the risk of receiving unwanted junk messages.

9.15 Subscriptions to email lists which are not WLDC approved are strictly prohibited. The volumes of messages that can be generated are high and there is no control over the content, which may conflict with the conditions stated above.

9.16 Email should not be used to send large attached files (i.e. 10 Megabytes or larger), unless very urgent. Many email systems including those used by other councils and government departments will not accept large files which are returned and may result in overloading WLDC's own email system. Secure file transfer such as SFTP or appropriately encrypted removable media should be used to send large amounts of data, whenever possible.

9.17 Attachments to email messages should not be opened unless they are expected. Extreme caution should be exercised.

9.18 The forwarding of WLDC business related information to personal email accounts is strictly prohibited and could result in disciplinary action being taken. The council provides a number of solutions for accessing the corporate email system when away from the office.

10 Internet and social media acceptable usage

10.1 WLDC will provide access to the internet including social media to all authorised employees, third parties, contractors and temporary staff to assist them in the performance of their jobs. Where access is provided, use should be limited to official council business. However, it is recognised that there may be occasions when employees, third parties, contractors and temporary staff would wish to use the internet and social media for personal reasons; this is permitted during your own time (i.e. you are allowed to browse the internet during breaks and lunches). The only social media channels the council will allow are Facebook, Twitter and Instagram. This personal usage must be kept to an absolute minimum. Any misuse of social media (e.g. excessive use) will be investigated in line with the Disciplinary Policy.

10.2 Applications to set up a social media account on behalf of the council must be processed by the Communications Team. Guidance is available to support staff who use social media channels on behalf of the council. For more information refer to the Social media Policy.

10.3 The use and viewing of internet based email (i.e. Yahoo mail and Gmail) is strictly prohibited.

10.4 Messages must not be posted on any internet message board, social networking sites or other similar web based services that could bring WLDC into disrepute, or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as that for email.

10.5 As part of routine security measures, all sites visited are centrally logged and monitored.

10.6 The internet and social media must not be used for illegal activities.

10.7 Internet access may not be used for personal financial gain nor should a website be hosted on any WLDC equipment without express permission.

10.8 The internet must not be used for participation in online games or the use of active web channels that broadcast frequent updates to PCs, such as the BBC News Ticker Tape services, streaming video or audio, for example, radio stations, unless specifically approved by the SIRO.

10.9 Websites that display material of a pornographic nature, or which contain material that may be considered offensive must not be accessed. It is recognised that accidental viewing of such material may happen from time to time, in this event the SIRO must be notified immediately.

10.10 Files from the internet, or any images that are displayed must not be downloaded for personal use. If a file is required from the internet ICT should be contacted - there may be any number of issues concerning copyright, viruses and overall functioning of the computer.

10.11 Email addresses must not be unnecessarily entered on a website. Disclosing email addresses when completing surveys or other questionnaires will increase the risk of receiving unwanted junk messages.

10.12 The person logged in at a computer will be considered to be the person browsing the internet. Remember to log out or lock computers if left unattended (press the “windows” key and the letter “L” key at the same time). Under no circumstances should the browsing of the Internet take place from a PC that is logged into the network by another person.

10.13 All internet access must be routed through the council’s internet proxy server.

10.14 WLDC monitors and logs all internet accesses by individuals and reserves the right to access and report on this information.

11 Telephone acceptable use policy

11.1 Personal calls should be kept to a minimum and not interfere with performance of duties. The council reserves the right to check, review and monitor telephone calls made using any council telephone or telephone system. Refer to the Telephone Monitoring Policy for more information.

11.2 Where the council provides a user with a mobile phone, it is to ensure that the user is contactable when away from the office. Therefore, council mobile phones should be switched on or directed to voicemail or an alternative phone at all times during working hours.

11.3 Voicemail should be checked regularly and greetings updated as necessary. Voicemail users should secure their messages with a minimum four-digit pin code and clear down messages on a frequent basis. Refer to the Customer Standards Handbook for more information.

11.4 To ensure that a mobile phone cannot be used fraudulently, it should be protected by using a PIN number. If a council mobile phone is lost or stolen it must be reported to the ICT Service Desk.

11.5 The council has a Code of Practice (see Appendix 1) relating to telephone use. This concerns the use of council-owned static and mobile telephones for private telephone calls and must be followed at all times.

11.6 Misuse of the council's telephone services is also considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action.

12 Clear screen and clear desk policy

12.1 The council has a clear desk policy in place to make sure that all information is held securely at all times. It also supports the council's flexible working arrangements.

12.2 Sensitive material must not be left in clear view on unattended desks.

12.3 At the end of each day, every desk must be cleared of all documents that contain any council OFFICIAL information, or any information relating to clients or citizens.

12.4 Trays containing work should be stored in a locked cabinet or drawer overnight, and there should be nothing left on desks at the end of the working day.

12.5 OFFICIAL-SENSITIVE information must be secured in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

12.6 Nothing should be left lying on printers, photocopiers or fax machines at the end of the day. Consideration should be given to the location of printers which are used for overnight printing. If OFFICIAL information is printed overnight then the printer is to be located in a secure location.

12.7 Users of IT facilities are responsible for safeguarding data by making sure that equipment is not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

12.8 Computer screens must be locked (press the “Windows” key + L) to prevent unauthorised access when unattended. Screens must lock automatically after a 5 minute period of inactivity in order to protect information. A screen saver with password protection enabled must be installed on all PCs and laptops. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action.

12.9 Floor space under furniture and around the office should remain free from obstructions at all times to facilitate the cleaning and maintenance of the building.

12.10 Checks of each area will be made regularly by team managers and any items that are found on the floor (apart from footrests and bins) will be removed.

12.11 As part of good housekeeping, boxes, folders etc. should not be stored on top of furniture, cabinets, window ledges etc.

12.12 Paper media containing payment card holder data must never be left unattended and must be locked in a secure storage facility.

12.13 The clear desk policy is not intended to hinder your day to day working. In an ideal world, we would all work with a clear desk.

13 Mobile device acceptable use policy

13.1 A Mobile Computing Device (MCD) (see the Mobile computing policy for a definition of an MCD) must never be left on view in a car, whether the vehicle is occupied or not.

13.2 A MCD must never be left unattended on any form of public transport or in bars/restaurants or any other public place.

13.3 Care must be taken when using MCDs in public places or unprotected areas outside of council premises to avoid the risk of information being overlooked or overheard.

13.4 The encryption utility must be enabled on all MCDs. This will prevent unauthorised access to data, even if the MCD is stolen. ICT can give advice regarding the protection of MCDs.

13.5 Anti-virus software must be up to date. Please contact the ICT department if unsure of current status.

13.6 MCDs must be kept secure as they could contain private and confidential information. The ICT department can give advice regarding safe storage of information on MCDs.

13.7 Smartphones are capable of collecting, storing and transmitting large quantities of data in many different formats. Council-supplied devices are encrypted, protected against malware and unauthorised access, and monitored for compliance. Users of smartphones issued by the council must make sure that they comply with relevant legislation, i.e. GDPR and DPA 2018, when capturing data using the device's camera or microphone.

13.8 Unless they have been secured and authorised for use under the council's Bring Your Own Device (BYOD) Policy, personal smartphones brought into council offices present a particular risk to data protection. Users should be aware that, in order to reduce the risk of data breaches, individual departments may choose to impose restrictions on the use of personal smartphones and similar devices in the workplace.

14 Responding to Security Incidents & Malfunctions

14.1 Any perceived or actual information security weakness or incident must be reported to the ICT Service Desk immediately. Examples of a security incident include unauthorised access to information assets, misuse of information assets, loss/theft of information assets, virus attacks, denial of service attacks, suspicious activity.

14.2 Further information on the reporting of security incidents can be found in the Information Security Incident Management Policy.

15 Validity of this policy

15.1 In applying this policy, WLDC will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

15.2 This policy must be reviewed when the need arises (i.e. when there are changes in the organisation or to relevant legislation). Reviews will be carried out by the Corporate Information Governance Group (CIGG) under the authority of the SIRO.

Appendix 1 – Creating good passwords

#ThinkRandom

1. Did you know that the password ‘123456’ has been found 23 million times in cyber security breaches? Proving that a common password will make you an easy target.

2. The NCSC has recommended **#ThinkRandom** for a few years and is still promoting this method of password creation.

3. Instead of creating extremely long and complex passwords, the NCSC’s **#ThinkRandom** recommends that, when setting up a password, users choose three random words. Examples used on the NCSC website are: ‘coffeetrainfish’ or ‘walltinshirt’.

4. Avoid using easy to guess passwords, such as ‘onetwothree’ or the names of family members or pets as this will make you an easy target for hackers.

Appendix 2 – Code of Practice Relating to Private Telephone Calls

This Code of Practice applies to the use of council-owned static and mobile telephones for private telephone calls.

Whenever possible, private calls should be made on an employee's personal device. However, the council acknowledges that employees may occasionally need to make calls of a personal nature using a council-owned device whilst at work. This Code of Practice outlines reasonable steps that all employees are expected to take to make sure that the provision of service is not compromised and there is no financial loss.

Where possible, private calls should be made outside standard hours of service provision, i.e. before 9pm, after 5pm, or during an employee's lunch break.

Private calls during these hours should be kept to a minimum, so as not to prevent business calls getting through.

Each employee should keep a record of the private calls they make. The council may carry out monitoring to ensure private use is not excessive.

There may be times when unforeseen working commitments may require the rearranging of personal engagements. The council recognises that such calls are necessary in order for employees to effectively perform their duties, and should not be treated as private. However, the council stresses that such calls are normally exceptional, and expect employees to recognise when such calls are required.

The council may, under certain circumstances, record telephone calls. Refer to the Telephone Recording Policy for more information.