Bolsover District Council,
Derbyshire Dales District Council
North East Derbyshire District Council
Dragonfly Developments Ltd

INFORMATION AND CYBER SECURITY POLICY

April 2024

CONTROL SHEET FOR Information and Cyber Security Policy

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	Information and Cyber Security
Status – i.e., first draft, version 2 or final version	April 2024 (updated 4/4/2024)
Policy author(s)	Assistant Director for ICT
Location of policy – i.e., L-drive, shared drive	NEDDC – TBC BDC – TBC DDDC – TBC Dragonfly - TBC
Member route for approval	NEDDC / BDC and DDDC Joint ICT Committee/Executive/ Cabinet
Cabinet Member (if applicable)	Cllrs Clive Moesby (BDC) and Cllr Joe Birkin (NEDDC)
Equality Impact Assessment approval date	In progress
Partnership involvement (if applicable)	In progress
Final policy approval route i.e., Executive/ Council /Planning Committee	Joint ICT Committee
Date policy approved	BDC 2024 NEDDC 2024 DDDC 2024
Date policy due for review (maximum three years)	April 2026
Date policy forwarded to Strategy and Performance (to include on Intranet)	2024

Contents

1 Introduction

North East Derbyshire District Council, Bolsover District Council, Derbyshire Dales District Council and Dragonfly Developments Ltd are dependent upon it's Information and Communications Technology (ICT) systems to ensure continued delivery of services to its customers. It is therefore essential for the continued successful operation of the district councils and Dragonfly Development Ltd. that the confidentiality, integrity and availability of its ICT systems and data are maintained at high levels at all times.

The information that the district councils, and Dragonfly Development Ltd. holds, processes, maintains, and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

To maintain public confidence and ensure that the district councils and Dragonfly Ltd. comply with relevant statutory legislation, it is vital that the councils and Dragonfly Ltd. maintain the highest standards of information and cybersecurity. As such, a number of policies are in place to maintain these high standards of information security; these are attached as appendices to this summary document. Member's requirements are covered in the Members ICT Charter.

2 Scope

For the purpose of this document, North East Derbyshire District Council, Bolsover District Council, Derbyshire Dales District Council and Dragonfly Development Ltd will be referred to as 'The Parties'.

This Information and Cyber Security Policy will apply to:

- all 'The Parties' employees, contractors, partners and agents, and other stakeholders such as contractual third parties, partners, agents, work placements and volunteers where they have access to ICT facilities and data.
- all assets owned by 'The Parties'.
- information held or owned, ICT infrastructure used and the physical environment in which the information and /or supporting ICT is used by 'The Parties'.
- employees and agents of other organizations who directly or indirectly support 'The Parties' IT services.
- 'The Parties' systems in hosted or cloud environments.

These policies are produced in line with guidelines and legislation that are available as of March 2024. These include:

2.1 Legislation and guidelines:

Copyright, Designs and Patents Act 1988 – downloading, copying, processing, or distributing information from the internet may be an infringement of copyright or other intellectual property rights.

Data Protection Act 2018, which covers the General Data Protection Regulations – care should be taken in the collection, processing or disclosure of any personal data and all personal data should be processed within the principles of the Act.

Information Commissioners Office (ICO) General Data Protection Regulations Guidance 1.0. This expands on the Data Protection Act

Human Rights Act 1998 – The HRA provides for the privacy of personal correspondence and the protection of that privacy while at work. Monitoring unless notified and done properly may infringe these rights.

Freedom of Information Act 2000 – all recorded information is potentially disclosable under the Act, including all expressions of fact, intent, and opinion. If a request for information is made, the Act prohibits destruction of the information until it is given out in response to the request. Please also see 'The Parties' guidelines on retention of information.

Public Services Network (PSN) Code of Connection. This is a requirement to access central government provided services and a comprehensive list of conditions must be met to achieve the requisite compliance.

3 Principles

This document provides a summary of the information and Cyber security policies developed for 'The Parties'. The objective of these policies is to ensure the highest standards of information security are always maintained across 'The Parties'.
so that:

- Duties are carried out in a professional and lawful manner and in accordance with 'The Parties' Codes of Conduct.
- The public and all users of 'The Parties' information systems are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- Customer and employee data is adequately protected, and the risk of data protection breaches reduced.
- All legislative and regulatory requirements are met.
- 'The Parties' ICT equipment and facilities are used responsibly, securely and with integrity at all times.

The guidelines aim to set out 'The Parties' policy on the use and monitoring of ICT and seek to strike a balance between users' right to privacy and 'The Parties' responsibility to ensure appropriate use of ICT.

Failure to comply with these guidelines may be viewed as a disciplinary matter and may, therefore, be subject to 'The Parties' agreed Disciplinary Procedures.

It is intended that from time to time, as is required by changes to legislation, technology or 'The Parties', these Guidelines will be subject to review. Any changes made will be subject to consultation and the changes communicated to users. By signing the agreement users are deemed to accept any revisions to this policy that are communicated to them.

4 Risks

'The Parties' recognise that there are risks associated with users accessing and handling information in order to conduct official 'The Parties' business. This policy aims to

mitigate those risks. Non-compliance with this policy could have a significant effect on the efficient operation of 'The Parties' and may result in financial loss and an inability to provide services to our customers.

5 Information Security Policy

The key areas of the policy are covered below:

- Protective Marking Policy
- Email Policy (Appendix 1)
- Internet Acceptable Usage Policy (Appendix 2)
- Software Policy (Appendix 3)
- ICT Access Policy (Appendix 4)
- Human Resources Information Security Standards (Appendix 5)
- Information Protection Policy (Appendix 6)
- Computer, Telephone and Desk Use Policy (Appendix 7)
- Remote Working Policy (Appendix 8)
- Removable Media Policy (Appendix 9)
- Information Security Incident Management Policy (Appendix 10)
- IT Infrastructure Policy (Appendix 11)
- WhatsApp Policy (Appendix 12)
- Microsoft Teams Policy (Appendix 13)
- Generative Artificial Intelligence Policy (AI) (Appendix 14)
- Data Protection
- Business Continuity
- Disposal and Destruction of Data
- Instant Messaging

A summary of the above as they apply to all users is included below, although employees should always refer to the relevant appendix for more detailed policy information.

5.1 Document Classification and Protective Marking Policy

Many organisations have formal documentation classification schemes. We have a responsibility to ensure we are aware of the data handling guidelines in relation to these documents or data. For these purposes documents are either paper whereas data is held in a business system database or as a raw data extract on 'The Parties' filing systems. Electronic documents would usually be created using part of the Microsoft Office suite or in 'pdf' format but other forms may also exist. If in doubt always seek clarification from the data owner or your line manager.

The 'Parties' have adopted the Government classification scheme. We should not receive any material classified as SECRET or TOP SECRET, any material classified as thus should be immediately deleted and the sender notified. There are two classifications that will apply to each organisation: OFFICIAL and OFFICIAL SENSITIVE:

- OFFICIAL-SENSITIVE Broadly this includes data or documents that contain personal sensitive data as defined by the Data Protection Act or defined under 'Special categories' under the General Data Protection Regulations. This can also include

items that would be considered exempt under the Freedom of Information Act in relation to commercial sensitivity.
- OFFICIAL Covers all other documents and data that do not fall under the OFFICIAL-SENSITIVE classification and will form most of the Councils data and documents.

A full definition of the Government Classification Scheme can be found at Government Classification Scheme - Security Guidance (justice.gov.uk)
Key points to note:

- New documents which contain personal sensitive data as defined by the Data Protection Act or fall within a 'Special Category' under the General Data Protection Regulations should be protectively marked as OFFICIAL-SENSITIVE on both the header and footer of each page.
- Amended documents should be protectively marked where not already marked
- Documents created in Microsoft Office should be protectively marked using sensitivity labels.
- Transmission of OFFICIAL-SENSITIVE material should be clearly marked as thus, and appropriate steps taken to ensure transmission is secure.
- Care should be taken with unmarked documents.

Under the General Data Protection Regulations in place from May 2018 the following are defined as 'Special Categories' of data or are covered elsewhere in the Regulation:

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data
- Biometric data
- Sex life or sexual orientation
- Physical and mental health
- Financial personal data
- Alleged criminal activity.
- Criminal record

5.2 Email (Appendix 1)

- The use of email facilities will be permitted only by users that have been specifically designated as authorised users, received appropriate training, and have confirmed in writing they accept and agree to abide by the terms of this policy.
- All emails that contain OFFICIAL-SENSITIVE information should be encrypted in transit when sent to other organisations whether in the public sector or not, see secure email guidance available on the ICT Help Section. Please contact the Joint ICT Service Desk if you are unsure if the recipient can receive secure email.
- Where correspondence is made directly with members of the public that contains OFFICIAL-SENSITIVE information it is not possible to ensure emails can be encrypted but all precautions to ensure the email address belongs to the intended recipient should be made.
- All correspondence which contains OFFICIAL-SENSITIVE material should be marked

using sensitivity labels.

- 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 council email and be protected accordingly.
- All official external e-mail must carry the official council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the equality legislation.
- Email should not be forwarded to personal email accounts under any circumstances.
- Auto forwarding of email-to-email addresses outside of 'The Parties' is not permitted.
- The legal status of an email message is like any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official 'The Parties' business should be considered as an official communication from 'The Parties'.
- 'The Parties' maintain their legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. 'The Parties' reserve the right, with written approval from an appropriate Director, Assistant Director or the Human Resources Manager, to monitor emails sent within the 'The Parties' email system without further notifying the individual concerned that the right is being exercised. Please see Appendix 1, specifically section 3.1, for further clarification on this issue.
- Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from 'The Parties' ICT systems.
- It should also be noted that email and attachments may need to be disclosed under current data protection legislation or the Freedom of Information Act 2000.

5.3 Internet Acceptable Usage (Appendix 2)

- Internet use is monitored by 'The Parties'.
- Users must familiarise themselves with the detail, essence, and spirit of the Internet Acceptable Usage policy before using the Internet facility provided.
- At the discretion of line manager, and provided it does not interfere with your work, 'The Parties' permit personal use of the Internet in your own time (for example during your lunch break).

- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.
- Any excess 'out of tariff' charges on 'The Parties' data contracts as a result of personal use must be reimbursed in full.

5.4 Software (Appendix 3)

- All software acquired must be approved by the ICT Servicedesk.

- Access to Cloud based or Software as a Service (SaaS) services must be approved by the Data protection Officer, ICT Management, and the Information Asset Owner.
- Under no circumstances should personal or unsolicited software be loaded onto 'The Parties' machine.
- Every piece of software is required to have a licence and 'The Parties' will not condone the use of software that does not have a licence.
- Unauthorised changes to software **must not** be made.
- Users are not permitted to bring software from home or download from the internet (or any other external source) and load it onto 'The Parties' devices unless this has been approved by the Joint ICT service.
- Users **must not** attempt to disable or reconfigure endpoint management software, anti-virus, proxy or firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

5.5 ICT Access (Appendix 4)

- All users must use strong passwords and where possible Multi Factor Authentication, see appendix 4 for details.
- Passwords must be always protected and must be changed at least every 120 days.
- It is a user responsibility to prevent their user ID and password being used to gain unauthorised access to 'The Parties' systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access 'The Parties' network without permission from the ICT Servicedesk.
- Partners or 3rd party suppliers must contact the Joint ICT Service before connecting to the 'The Parties' network.

5.6 Human Resources Information Security Standards (Appendix 5)

- All employees are expected to adhere to this policy.
- Access to Information systems must be relevant to the jobholder's role and duties
- All mandatory ICT training should be completed in a timely manner or access to systems will be removed.
- In addition to normal recruitment verification checks carried out on all new employees' additional checks may be required, primarily when accessing systems and data provided by 3rd parties.

5.7 Information Protection Policy (Appendix 6)

- 'The Parties' must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the Government Security Classification scheme.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until their Line Manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

- OFFICIAL-SENSITIVE information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing OFFICIAL-SENSITIVE classified information to any external organisation is also prohibited, unless via secure email.
- The disclosure of OFFICIAL-SENSITIVE information other than for approved purposes is a potential breach of current Data Protection legislation and should be reported to the internal Data protection team.

5.8 Computer, Telephone and Desk Use (Appendix 7)

- Users must adhere to any 'The Parties' Computer, Telephone and Desk Use Policies that may be in force.
- Users should aim to maintain a clear desk at all times.
- 'The Parties' OFFICIAL-SENSITIVE information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

5.9 Remote Working (Appendix 8)

- It is the users' responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention. Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- All OFFICIAL-SENSITIVE data held on portable computer devices must be encrypted.

5.10 Removable Media (Appendix 9)

- The use of all removable media devices such as USB memory sticks, data cards and writeable CD's and DVDs is prohibited unless a business case is agreed, training given, and agreement signed to this effect.
- Any removable media device that has not been supplied by IT **must not** be used.
- All data stored on removable media devices **must** be encrypted where possible, and personal data must not be stored on devices that are not encrypted. Only data that is authorised and necessary to be transferred should be saved on to the removable media device. N.B. Data that has been deleted can still be retrieved.
- Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.
- Damaged or faulty removable media devices must not be used.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. 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.
- Removable media devices that are no longer required, or have become damaged, must be taken to the IT section for secure disposal.
- Laptops should remain with staff when they leave the office, this supports business continuity in the event of adverse weather and any issues with access to office buildings.

- If a laptop must be left in the office overnight or at weekends these should be placed out of sight preferably in a locked drawer or cupboard.
- Users should be aware of their responsibilities in regard to current data protection legislation and report any suspected breaches.

5.11 Information Security Incident Management (Appendix 10)

- All users should report any incidents or suspected incidents immediately by contacting the Joint ICT Service.
- Anonymity when reporting an incident can be maintained if desired.
- Phishing - If you are unsure whether an email, weblink or attachment is legitimate you should contact the Servicedesk for advice. If you have clicked on an email, link, opened an attachment or entered credentials and it doesn't seem right, contact the Servicedesk for advice, to help remedy the situation and prevent it impacting others.
- If an incident requires information to be collected for an investigation, strict rules must be adhered to. The Data Protection team should be contacted for guidance.
- Users should be aware of their responsibilities in regard to current data protection legislation and report any suspected breaches.

5.12 ICT Infrastructure Security (Appendix 11)

- OFFICIAL-SENSITIVE information, and equipment used to store and process this information, must be **stored** securely.
- Desktop PCs should not have data stored on the local hard drive.
- Non-electronic information must be assigned an owner and a classification. OFFICIAL-SENSITIVE information must have appropriate information security controls in place to protect it.
- Users should be aware of their responsibilities regarding current data protection legislation and report any suspected breaches.
- Equipment that is to be reused or disposed of must be returned to ICT to have all of its **data and software erased / destroyed**.

5.13 WhatsApp Policy (Appendix 12)

- Microsoft Teams is 'The Parties' approved corporate communication tool and should be used wherever possible. However, 'The Parties' accept that for the specific purpose of business continuity WhatsApp is a useful collaboration tool.
- WhatsApp can be installed on corporate mobile phones with approval from a senior manager.
- WhatsApp must only be used for business continuity purposes such as:
    - To provide information on office closures, urgent council updates to employees who do not have access to email or Microsoft Teams.
    - To inform colleagues or managers that you are unable to attend the office.
    - Arranging shifts etc, with casual staff who do not have access to other corporate communication.
    - It should not be used to communicate with the public unless this has been explicitly approved by the data protection officer and ICT Management.
- Under **no circumstances** should any **Official-Sensitive** data be shared via WhatsApp Discussions on council issues or workload should be conducted by phone, in 1 to 1's or team meetings and email.

- It is the responsibility of the user to ensure that the group membership on WhatsApp is kept up to date and the information is shared to the correct recipients.

5.14 Microsoft Teams Policy (Appendix 13)

- Microsoft Teams is the approved corporate collaboration tool and enables you and your colleagues to send instant messages, make video and audio calls, share, and edit files as a team and with external partners where appropriate.
- Microsoft Teams can and should only be accessed by corporately managed devices such as laptops, virtual desktops mobile phones and tablet devices such as iPads.
- When sharing information, you should always check the membership of the Team or Channel you are collaborating with.
- Default retention policies are in place for chats and Teams.
- Teams Site owners are accountable for ensuring that any of their information assets or extracts are managed appropriately within Microsoft Teams.
- Users should be aware that all Teams usage is monitored and recorded centrally.
- Teams and OneDrive provides the ability to share files with other members of the Team, you are responsible for ensuring that files are only shared to the appropriate people within the team and that files should have the appropriate protective marking applied (official or official-sensitive).
- You should ensure that chats within Teams Channels are used in an appropriate manner and follow council policies on appropriate behaviour.
- OneDrive and Teams can be used to share files, however until cloud backups have been implemented, you should keep copies of the original files on the S or X drive.
- You are responsible for ensuring the files are only shared to the appropriate people.

5.15 Generative Artificial Intelligence (AI) (Appendix 14)

- Generative artificial intelligence (GenAI) can produce a range of useful outputs, like text, audio, images, and code very quickly and easily.
- 'The Parties' acknowledge the benefits of utilising GenAI to improve efficiencies and effectiveness.
- However, 'The Parties' also acknowledge that there are many risks associated with using these technologies such as:
    - loss of data, personal / official-sensitive data
    - equalities issues, due to bias or discrimination
    - production of inaccurate or misinformation
    - legal compliance, for example copyright infringement.
- GenAI is already built into some of the Microsoft applications available on 'The Parties' IT systems, such as the Bing search engine within the Microsoft Edge browser and within some Microsoft 365 applications.
- Before using any GenAI tools available to 'The Parties', users must acknowledge that they have read and understood the guidelines in the Generative AI Policy found in Appendix 14.
- Sensitive or confidential (official-sensitive) data should not be entered into public GenAI tools.

5.16 Data Protection

- All employees are expected to adhere to 'The Parties' Data Protection practices and the specific policies listed supports compliance with current data protection legislation and reduces the risk of data protection breaches.
- Full details and guidance are available on the Data Protection pages on the 'The Parties' Intranet.

5.17 Business Continuity

Electronic information assets are protected to ensure 'The Parties' business can continue in the event of significant physical disruption to one or more of 'The Parties' sites. This includes:

- Physical security, arms and fire suppressant at main data centres
- Daily replication of data to designated disaster recovery sites for data managed by the Joint ICT Service
- Daily backups of data held offsite for data managed by the Joint ICT Service. This data is retained for 30 days
- Immutable backups retained for 6 months.
- Corporate business continuity plans

5.18 Disposal and Destruction of Data

- Confidential waste bins are provided for the secure destruction of paper based records.
- All unused electronic devices should be returned to the Joint ICT Service when no longer in use.
- All Council electronic data devices and removable are disposed of by the Joint ICT Service in accordance with regulation and for removable media and hard disks are destroyed to DOD 5220-22M standard
- Please refer to 'The Parties' Corporate Retention & Disposal Schedules

5.19 Instant Messaging

- Some business applications now include the facility for 'Instant Messaging' (IM) between other users of the system.
- Any communications made by IM should be for business purposes only.
- 'The Parties' maintain their legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of IM by authorised users to ensure adherence to this Policy. 'The Parties' reserve the right, with written approval from an appropriate Director, Assistant Director or the Human Resources & OD Manager, to monitor IM sent within 'The Parties' business systems without further notifying the individual concerned that the right is being exercised.

6 Responsibility for Implementation

The following table identifies who within 'The Parties' is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Assistant Director ICT
Accountable	Section 151 Officer
Consulted	Human Resources, Data Protection Officers, Scrutiny, Consultative groups (UECG, JCG).
Informed	'The Parties' users as defined in the scope

7 Policy Compliance

All users will be required to undertake an on-line ICT Induction and electronically sign a declaration confirming they have received the training and confirm they will abide by the ICT Policies.

If any user is found to have breached this, or any policy contained within the Appendices attached, they will be subject to 'The Parties' disciplinary procedure, as appropriate. For contracted 3rd parties this would be dealt by the employing authority in accordance with their own disciplinary procedures. If a criminal offence is considered to have been committed the Council will support any action to assist in the prosecution of the offender(s).

If you do not understand the implications of this, or any policy contained within the Appendices attached, or how they may apply to you, seek advice from your line manager.

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy.
- Unauthorised disclosure or viewing of confidential data or information belonging to 'The Parties'.
- Unauthorised changes to information, software, or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body.

- The exposure of 'The Parties' to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information Security Manager or their department or service manager.

8 Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the circumstances of the incident in question.

- If complying with the policy would cause significant damage to 'The Parties' reputation or ability to operate
- If complying with the policy would breach Health and Safety.
- If an emergency, within the context of the emergency plan, arises.

In such cases, the user concerned must take the following action:

- Ensure that a 'The Parties' manager is aware of the situation and the action to be taken.
- Ensure that the situation and the actions taken are recorded in as much detail as possible and reported to the ICT Service Desk.
- Ensure that the situation is reported to the Information Security Manager as soon as possible.
- Failure to take these steps may result in disciplinary action.

In addition, ICT maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified.
- Minor breaches that are not considered to be worth rectifying.
- Any situations to which the policy is not considered applicable.

'The Parties' will take no disciplinary action in relation to known, authorised exceptions to the information security management system.

This policy will be included within 'The Parties' Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.

9 Glossary of terms

Public Services Network (PSN) - This is a secure wide area network (WAN) that allows access to Central Government systems, secure data transfer, secure email and accredited solutions provided by public sector organisations and accredited 3rd parties. At present this includes CIS(Benefits) and WURTI. The scope of the PSN network covers local authorities, central government departments, National Health Service, the Criminal Justice Extranet, and the Police National Network.

Government Security Classifications – a marking scheme of information assets as used by the UK Government. Details of this scheme can be found via https://www.gov.uk/government/publications/government-security-classifications and the new marking classification guidelines can be found in Appendix A.

10 Contact Information

At the time of publication of this policy

the **ICT Servicedesk** is available on:-

- **Self Service portal > http://sworksrv.ne-derbyshire.gov.uk/sw/selfservice/**
- **Email : -** **servicedesk@ne-derbyshire.gov.uk**
  servicedesk@bolsover.gov.uk
  servicedesk@derbyshiredales.gov.uk
- **Telephone : - 3001 or 01246 217103**
- **Monday to Friday 08:00am – 5:30pm**

For incidents outside of these hours please contact the Information Security Manager who is the Assistant Director for ICT.

APPENDIX 1 - E-MAIL POLICY

1. Introduction

'The Parties' will ensure all users of 'The Parties' email facilities are aware of the acceptable use of such facilities.
The Policy establishes a framework within which users of 'The Parties' email facilities can apply self-regulation to their use of email as a communication and recording tool.

2. Scope

This policy covers all email systems and facilities that are provided by the 'The Parties' for the purpose of conducting and supporting official business activity through 'The Parties' network infrastructure and all stand alone and portable computer devices.
This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees, and individuals working on behalf of 'The Parties' contractual third parties and agents, work experience and volunteers, who have been designated as authorised users of email facilities.
The use of email facilities will be permitted only by users that have been specifically designated as authorised users for that purpose, received appropriate training and have confirmed in writing that they accept and agree to abide by the terms of this policy.
The use of email facilities by users that have not been authorised for that purpose will be regarded as a disciplinary offence.
The policies are based on industry good practice and intend to satisfy the requirements set out by the Public Service Network Code of Connection.
References to protective marking schemes and guidance on assessing and handling such information are covered in Section 5.1 of the Information Security Policy

3. Email Policy

3.1 Email as Records

- All emails that are used to conduct or support the councils business must be sent using a "@<council>.gov.uk" address. All emails that are used to conduct or support official Dragonfly Development Ltd. business must be sent using a "@dragonfly-uk.net" 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 'The Parties' email and be protected accordingly.
- All official external e-mail must carry the official 'The Parties' disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with equality legislation.
- For OFFICIAL-SENSITIVE information encryption **should** be used for all content and/or attachments that contain that classification. Secure email guidance is available on 'The Parties' Intranet.
- Where secure email is **not** available to connect the sender and receiver of the email message, and information classified as OFFICIAL-SENSITIVE is being transferred, alternative encryption methods **must** be used for all content and/or attachments that contain that classification. The ICT Service Desk will advise on options available.
- Emails carrying OFFICIAL-SENSITIVE contents and/or attachments must be labelled

to highlight the sensitivity and value that the information has to the data owner. This will be in the format of the Subject Header containing the label "OFFICIAL-SENSITIVE" as appropriate.

- Auto forwarding of email to email addresses outside of 'The Parties' is not permitted.
- Automatic forwarding of email within the organisations email system must be considered carefully to prevent OFFICIAL-SENSITIVE material being forwarded inappropriately.
- When handling data and documents provided by a 3rd party any document handling guidance provided by the 3rd party should be observed.

Non-work email accounts **must not** be used to conduct or support official 'The Parties' business. Users must ensure that any emails containing sensitive information must be sent from an official 'The Parties' email. Any 'The Parties' emails containing OFFICIAL-SENSITIVE information must be sent via secure email. All emails that represent aspects of 'The Parties' business or 'The Parties' administrative arrangements are the property of 'The Parties', as appropriate, and not of any individual employee.
Emails held on 'The Parties' equipment are considered to be part of the corporate record and email also provides a record of user's activities.
The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official 'The Parties' business should be considered to be an official communication from 'The Parties'. To ensure that 'The Parties' is protected adequately from misuse of e-mail, the following controls will be exercised:

i. It is a condition of acceptance of this policy that users comply with the instructions given during the email training sessions.
ii. All official external e-mail must carry the following disclaimer:

> *"Disclaimer*
> *This email is confidential, may be legally privileged and contain personal views that are not the views of* <insert 'The Parties' name>.
> *It is intended solely for the addressee. If this email was sent in error please notify the sender, delete the email and do not disclose, copy, distribute, or rely on it. Under the Data Protection Act 1998 and the Freedom of Information Act 2000 the contents of this email may be disclosed.*
> *This message and attached files have been virus scanned.*
> *Attachments are opened at your own risk."*

Whilst respecting the privacy of authorised users, 'The Parties' maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. 'The Parties' reserves the right, with written approval from an appropriate Director or Assistant Director or the Human Resources & OD Manager, to monitor emails sent within 'The Parties' email system (including personal emails) and to access mailboxes

and private directories without further notifying the individual concerned that the right is being exercised.
'The Parties' may exercise this right, with approval from an appropriate Director, Assistant Director or Human Resources & OD Manager and in accordance with the Data Protection Policy, in order to establish facts relevant to 'The Parties' business and to comply with:

- regulatory practices or procedures,
- to prevent or detect crime,
- to ensure compliance with 'The Parties' policies,
- to investigate or detect unauthorised uses of the system or to ensure the effective operation of the system (e.g. to check if viruses are being transmitted).
- to ensure critical work or urgent items can be actioned.
- disclosure under current data protection legislation or the Freedom of Information Act.

In these circumstances you do not have a right to privacy when using 'The Parties' information systems or in relation to any communication generated, received or stored on the 'The Parties' information systems.
These actions will be supervised by the Information Security Manager.
Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from 'The Parties' systems.
It should also be noted that email and attachments may need to be disclosed under current data protection legislation or the Freedom of Information Act 2000. Further information regarding this can be obtained from the appropriate Data Protection Officer.

3.2 Email as a Form of Communication

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, nor 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 OFFICIAL-SENSITIVE information or of communicating in the particular circumstances.
All emails sent to conduct or support official 'The Parties' business must comply with corporate communications standards. 'The Parties' Communications and Operation Management Policy must be applied to email communications.
Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on 'The Parties' reputation or its relationship with customers, clients or business partners.
When sending emails internally or externally the user should exercise due care in selecting the recipients to send the communication to. This is particularly important when sending personal and sensitive data.
Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the 'The Parties' Equal Opportunities Policies, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any

material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by 'The Parties' for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of OFFICIAL-SENSITIVE material concerning the activities of 'The Parties'.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste users effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission 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.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, marital status, disability, political, religion or belief, maternity or paternity, civil partnership, gender reassignment or sexual orientation.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council or Rykneld Homes Ltd into disrepute.

3.3 Unsolicited Mail

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

Before giving your e-mail 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 e-mails (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 'The Parties' systems or facilities.

3.4 Mail Retention

To ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addresses is discouraged.
Whilst there are no limits on mailbox sizes emails will automatically be deleted after 2 years.
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 is to avoid excessive use of the system and avoids filling to capacity another person's mailbox.

3.5 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that the 'The Parties':

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.
- Can respond to a formal complaint.

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

a. Establishing the existence of facts relevant to the business, client, supplier and related matters.
b. Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
c. Preventing or detecting crime.
d. Investigating or detecting unauthorised use of email facilities.
e. Ensuring effective operation of email facilities.
f. Determining if communications are relevant to the business.
g. It should also be noted that email and attachments may need to be disclosed under current data protection legislation or the Freedom of Information Act 2000.

Where a manager suspects that the email facilities are being abused by a user, they should contact the ICT Management and HR. Designated staff in the Joint ICT Service can provide evidence and audit trails of access to systems. The Joint ICT Service will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee'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 the latter is the case the Councils or Rykneld Homes Ltd may exercise this right, with approval from an appropriate Director, Assistant Director or the Human Resources & OD Manager. This 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.

3.6 Classification of Messages

The Council has adopted the Government protective marking scheme. However, we may handle data on behalf of 3rd parties who, as data owners, have adopted different protective marking schemes and data handling guidance. Please refer to section 5. of the Information Security Policy for further information.

3.7 Secure email

Emails sent between:

ne-derbyshire.gov.uk,
bolsover.gov.uk and
derbyshiredales.gov.uk
dragonfly-net.uk

addresses are held with the corporately managed networks and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, OFFICIAL-SENSITIVE material must not be sent via email unless assured as secure.
Where secure email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating OFFICIAL-SENSITIVE material.
Where secure email is not available to connect to the receiver of the email message, and information classified as OFFICIAL-SENSITIVE is being transferred, encryption should be used for all content and/or attachments that contain that classification. Please contact the Service Desk if you are unsure the recipient can receive secure email.
Emails carrying OFFICIAL-SENSITIVE contents and/or attachments must be labelled to highlight the sensitivity and value that the information has to the data owner. This will be in the format of the Subject Header containing the label "OFFICIAL-SENSITIVE" (with appropriate descriptor) as appropriate.
Please refer to the secure email guidance available on the Joint ICT Service Intranet.

3.8 Confidentiality

All users 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 (customers and employees). If any user is unsure of whether they should pass on information, they should consult the relevant Data Protection Officer.

Users must make every effort to ensure that the confidentiality of email is appropriately maintained. Users should 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 outside 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 'The Parties'.
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) must be considered carefully to prevent OFFICIAL-SENSITIVE material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the ICT Servicedesk in the first instance.

3.9 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. If any user has concerns about possible virus transmission, they must report the concern to the Joint ICT Service and under no circumstance forward emails and attachments or open links in an email if there is any cause for concern.
In particular, users:

- Must not transmit by email any file attachments which they know 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 'The Parties' facilities.
- Must not forward virus warnings other than to the ICT Servicedesk.
- Must report any suspected files to the ICT Servicedesk.

In addition, 'The Parties' will ensure that email is virus checked at the network boundary and at the host.
If a computer virus is transmitted to another organisation, 'The Parties' could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

3.10 Phishing

Phishing emails are a form of social engineering and scam where attackers try to deceive people into revealing sensitive information, transferring money, or installing malware such as ransomware. Phishing attacks have become increasingly sophisticated and can be difficult to spot, however it is important that users of 'The Parties' email systems become familiar with common Phishing tactics, how to spot them and what to do if you do get Phished.
Emails sent from outside of 'The Parties' email system should display the text 'Warning External'.

Phishing Emails often have an urgency to them, propose to come from someone with authority, may be too good to be true, contain links or attachments.
Carefully check the address the email originated from, confirm links are legitimate by going direct to the known companies' website. If in doubt, contact the Joint ICT Servicedesk who will be able to offer advice.
If you have responded, opened, or clicked a link contained within an email which looks suspicious, report this to the Joint ICT ServiceDesk as soon as possible as they can help to fix things and to stop it happening again to you or anyone else.

APPENDIX 2 - INTERNET ACCEPTABLE USAGE POLICY

1. Introduction

'The Parties' provide many and diverse Information and Communications Technology ("ICT") services, tools and equipment to employees to be used in the course of their work, including computers, laptops, telephones, internet and email.

The internet has become a fundamental tool which 'The Parties' use for research and education purposes.

'The Parties' support information and communications resources which will enhance the business and service environment. However, with access to computers and people all over the world via ICT comes the availability of material that may not be considered of value in the context of 'The Parties' setting. Additionally, as with any resource, there is the possibility of misuse. Accordingly, the Council and Rykneld Homes need to set guidelines for the use of ICT and, where appropriate, to monitor its use.

However, even with the guidelines, 'The Parties' cannot prevent the possibility that some users may access material, even inadvertently, that is not consistent with the policies of 'The Parties' or in line with the normal duties and responsibilities of the user.

2. Scope

All information, whether electronic or paper based, relating to our customers, suppliers and business operations should be treated in line with (a) 'The Parties' Code of Conduct for Members and Officers, (b) relevant policies and (c) relevant legislation.

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who make use of the internet.

4. What is the Purpose of Providing the Internet Service?

4.1 General guidelines on use of the internet

Use of the Internet is available at your line manager's discretion. In general, users shall only use the Internet for official purposes, e.g., access to and the provision of information, research, electronic commerce. Use of information from the Internet shall be directly related to the official duties of the user, or 'The Parties' as a whole. All information downloaded from the Internet shall be related to the duties and tasks of the user. However, reasonable personal use is permitted within a user's own time at the discretion of their line manager.

Where there is public access to the Internet provided by 'The Parties' and a member of the public misuses this provision, it will not be deemed to be the responsibility of any employee present at the time. However, the employee should report this incident as a breach of security to ICT.

Any information distributed or released by users by way of the Internet is subject to 'The Parties' guidance on the release of information and shall, prior to such distribution, be approved by the relevant management procedures.

Any proposed links from 'The Parties' Internet sites to the other Internet sites must first be authorised by a member of the senior management team.

Users must be aware that the quality and accuracy of information available on the Internet is variable. It is the responsibility of the individual user to judge whether the

information obtained is satisfactory for the purpose for which it will be used, and, if appropriate, steps should be taken to verify this information independently.

Where the Internet is being accessed by employees via a mobile device (laptop or tablet, or smartphone) from an internet connection which is not covered by 'The Parties' internet filtering software, the same guidelines on appropriate use of the Internet apply and extra care must be taken not to visit sites which would be deemed unsuitable.

4.2 Specific Guidelines on Use of the Internet

- Software, must not be downloaded from the Internet by users without the advice and permission of ICT personnel.
- When participating in newsgroups or mailing lists, users may offer information and advice to others if it is appropriate to their official duties or tasks or if the benefit to be gained by 'The Parties' represents a reasonable return in terms of the effort involved.
- Employees must not take part in discussions on political matters via the Internet unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited trade union representative.
- Users must not use their access to the Internet for their own private business purposes.
- Orders for goods purchased for 'The Parties' purposes must not be placed by way of the Internet without the employee having first obtained approval from their line manager, having authorised the purchase in the normal departmental manner and having complied with 'The Parties' Contract Standing Orders and Financial Regulations.
- Users must not use 'The Parties' Internet facility for the purpose of gambling.
- Users must not break or attempt to break any system security controls placed on their Internet Account.
- Users must not intentionally access or transmit computer viruses or software programs used to trigger these.
- Users must not intentionally access or transmit information which is obscene, sexually explicit, racist, or defamatory or which depicts violent or criminal acts or otherwise represents values that are contrary to 'The Parties' policy.
- Employees must not intentionally access or transmit information of a political nature unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited trade union representative.
- Users must not knowingly break the law.
- If an Internet site containing unsuitable material e.g., of an obscene nature is inadvertently accessed by a user, this must be immediately reported to ICT as a security breach.
- If material is inadvertently accessed which is believed to contain a computer virus, the user must immediately break the connection to the Internet and contact ICT for advice and assistance.
- Users must not copy information originating from others and re-post it without the permission of or acknowledgement to the original source.

5. Personal Use of the Internet Service

Any reasonable personal use of 'The Parties' ICT services and equipment must comply with 'The Parties' Code of Conduct for Officers and Members. Reasonable personal use of such services and equipment:-

- Must not be carried out in works time
- Must not interfere with the performance of your duties.
- Must not take priority over your work responsibilities
- Must not result in 'The Parties' incurring expense
- Must not have a negative impact on 'The Parties' .
- Must be lawful and in accordance with 'The Parties' Policy and with the guidelines as set out in this document.

Where reasonable personal use is referred to in this document, this section applies.
Reasonable personal use of 'The Parties' internet service is permitted only in the employee's own time (i.e. before clocking on, or after clocking off in accordance with the appropriate flexi-time Scheme).
Please refer to any local policies with regards to excess or 'out of tariff' charges incurred on 'The Parties' provided broadband or mobile data contracts. .

6. Internet Account Management, Security and Monitoring

6.1 Monitoring and Reporting Internet Use

All access to the Internet is automatically logged against an identifier unique to the device of the user, is recorded and may be monitored by 'The Parties'. This monitoring will be for the prevention and detection of unauthorised use of 'The Parties' communication systems.

Auditable statistics are kept within ICT of all 'The Parties' *Internet access.*

Line managers are able to access details of sites visited by employees and the time spent accessing the internet. Such reporting is not provided on a set basis, but will be available to managers in the normal course of an investigation into inappropriate or prolonged use of the Internet by a user.
'The Parties' actively monitors access to inappropriate sites via the Internet security software. Any 'irregularities' encountered in this process are reported to the line manager of an employee in accordance with 'The Parties' policies.
'The Parties' in the case of an investigation requiring to be carried out into the use of Internet access by a user, the relevant authority (this will be the line manager and/or Human Resources in the cases of an employee) will contact the Joint ICT Service who will access the necessary monitored information and provide a report of this to the relevant authority.
Internet filtering software is used to block access to sites which have been deemed unacceptable. In certain cases, where authorised by a line manager, users in specific posts may be allowed access to sites normally blocked to users where access to sites is required or helpful in the undertaking of the duties of the post.

7. Things You Must Not Do

Access to the following categories of websites is currently blocked using a URL filtering system:

- Pornography/Sexually Explicit/Sex Education/Nudity
- Child Abuse Images
- Hate and Intolerance
- Violence and Weapons
- Self Harm

- Hacking/Peer-to-peer
- Tasteless
- Illegal Drugs/Gambling
- Download sites.
- Terrorism
- Games/Downloads
- Illegal/Criminal activity
- Religious extremism / Cults
- Newly registered domains
- Games

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet account to:

- Create, download, upload, display, or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Run a private business.
- Use non-corporate chat or instant messaging platforms (WhatsApp, etc.).
- Download any software that does not comply with 'The Parties' policies.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and 'The Parties' policies.

8. Your Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence, and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use 'The Parties' Internet facility within the terms described herein.
- Read and abide by the following related policies:
    - Email Policy. (see Appendix 1)
    - Software Policy. (see Appendix 3)
    - IT Security Policy. (see Summary)

9. Whom Should I Ask if I Have Any Questions?

In the first instance you should refer questions about this policy to your Line Manager who will refer you to an appropriate contact. You should refer technical queries about 'The Parties' Internet service to IT Management.

APPENDIX 3 - SOFTWARE POLICY

1. Introduction

'The Parties' will ensure the acceptable use of software by all users of 'The Parties' computer equipment or information systems.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who make use of ICT equipment.

3. Software Policy

This policy should be always applied whenever using 'The Parties' computer equipment or Information systems.

3.1 Software Acquisition

All software acquired by 'The Parties' may only be purchased following consultation with the joint ICT service and approval provided by ICT management. Software may not be purchased through user corporate credit cards, petty cash, travel, or entertainment budgets. Software acquisition channels are restricted to ensure that 'The Parties' has a complete record of all software that has been purchased and installed and can register support and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto 'The Parties' devices as this may affect the performance of your device and the risk of introducing a virus.

3.2 Cloud or Software as a Service (SaaS) Acquisition

The authority may be required to use Cloud based software or Software as a Service (SaaS), often accessed via an internet Browser. Before procuring or using cloud-based software or Software as a Service (SaaS) a Data impact assessment (DPIA) must be completed with advice from the Data Protection Officer. ICT must also be informed so a risk assessment of the cloud service can be completed. Where the service stores or processes personal-sensitive data, a full security assessment must be completed by the vendor and submitted to ICT for review. The data owner will be informed of any recommendations from the assessment before they make an informed decision based on whether to continue with the procurement and use the services.

Cloud based systems should only be accessed using corporately managed devices unless pre-authorised by the data protection officer.

4.2 Software Registration

'The Parties' use software in all aspects of its business to support the work carried out by its employees. In all instances every piece of software is required to have a licence and 'The Parties' will not condone the use of any software that does not have a licence. Software must be registered in the name of 'The Parties' and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The Joint ICT Service maintains 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 location of each installation as well as the serial number of the hardware on which each copy of the software is installed.
d) The existence and location of back-up copies.
e) The software product's serial number.
f) Details and duration of support arrangements for software upgrades.

Software on local area networks or multiple machines shall only be used in accordance with the licence agreement.
'The Parties' hold licences for the use of a variety of software products on 'The Parties' Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer.
It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

4.3 Software Installation

Software must only be installed by the Joint ICT Service once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by the Joint ICT Service.
Software may not be used unless approved by ICT management, or their nominated representative.
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 onto 'The Parties' systems without prior approval from Joint ICT Service
To maintain PSN compliance and to mitigate the risk of security vulnerabilities only versions of software that are supported by the manufacturer of that software will be permitted. Where applicable a current support and maintenance agreement with the application provider should be in place.

4.4 Software Development

All software, systems, and data development for 'The Parties' is to be used only for the purposes of 'The Parties'.
Software must not be changed or altered by any user unless there is a clear business need and approved by ICT Management. 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:

1. Change requests affecting a software asset should be approved by the software asset's owner.
2. All change requests should consider whether the change is likely to affect existing security arrangements, and these should then be approved.
3. A record should be maintained of agreed authorisation levels.
4. A record should also be maintained of all changes made to software.
5. Changes to software that have to be made before the authorisation can be granted should be controlled.

4.6 Software Misuse

'The Parties' will ensure that Firewalls and antivirus products are installed where appropriate. Users **must not** attempt to disable or reconfigure the Firewall or anti-virus software.

It is the responsibility of 'The Parties' users to report any known software misuse to the Joint ICT Service.

According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any individual, who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under the circumstances. Any illegal duplication of software may be treated as a disciplinary offence.

APPENDIX 4 - ICT ACCESS POLICY

1. Introduction

Access control rules and procedures are required to regulate who can access 'The Parties' information resources or systems and the associated access privileges. This policy always applies and should be adhered to whenever accessing 'The Parties' information in any format, and on any device.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who access ICT services.

3. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally, or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

4. Applying the Policy - Passwords

4.1 Choosing passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

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

Weak and strong passwords

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 words that may be present in a 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.

Strong passwords should be used with a minimum standard of:

- At least twelve characters.
- Contain a mix of alpha and numeric, with at least one digit
- Contain a mix of upper and lower case with at least one upper case character.
- Contain special characters such as @?#.,

Where possible Multifactor authentication should be enabled, especially when accessing systems hosted in the cloud.

Conditional access controls should also be implemented where possible when accessing cloud-based systems which restrict access either to corporate devices or the Corporate network.

4.2 Protecting Passwords

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 passwords to anyone.
- 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 within the password.
- Do not use the same password for multiple systems.

4.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 120 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the Joint ICT Service.

Users **must not** reuse the same password within 20 password changes.

5. System Administration Standards

'The Parties' IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users- i.e., no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.
- Regular review of user access rights and privileged access rights.

6. Applying the Policy – Employee Access

6.1 User Registration

A request for access to 'The Parties' computer systems must first be submitted to the Joint ICT Service for approval. Applications for access must only be submitted if approval has been gained from your line manager.

When a user leaves 'The Parties', their access to computer systems and data must be suspended at the close of business on the user's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the Joint ICT Service and the relevant business system administrators.

6.2 User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to 'The Parties' systems by:

- Following the password policy and statements outlined above.
- Ensuring that any device they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the Joint ICT Service and the relevant business system administrators of any changes to their role and access requirements.

6.3 Network Access Control

Connecting non corporately managed devices to 'The Parties' networks is strictly forbidden without prior approval and risk assessment by the Joint ICT Service.

7. Users Authentication for External Connections

Where remote access to 'The Parties' network is required, an application must be made to the Joint ICT Service. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a biometric device or authentication token. For further information please refer to the Remote Working Policy (Appendix 9).

7.1 Supplier's Remote Access to the Network

Partner agencies or 3rd party suppliers must not be given details of how to access 'The Parties' network without permission from the Joint ICT Service. Any changes to supplier's connections must be immediately sent to the Joint ICT Service so that access can be updated or ceased. All permissions and access methods must be controlled by the Joint ICT Service.

Partners or 3rd party suppliers must contact the Joint ICT Service before connecting to 'The Parties' network and a log of activity must be maintained. Remote access software must be disabled when not in use.

APPENDIX 5 - HUMAN RESOURCES INFORMATION SECURITY STANDARDS POLICY

1. Introduction

'The Parties' hold large amounts of personal and protectively marked information. Information security is very important to help protect the interests and confidentiality of 'The Parties' and their customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

2. Scope

This policy applies to all users that require access to 'The Parties' information systems or information of any type or format (paper or electronic).

The definition of users within this policy is intended to include all Services, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who have access to ICT equipment.

Where access is to be granted to any third party (e.g., contractors, service providers, voluntary agencies, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with 'The Parties' user that initiates this third-party access.

3. Principles

'The Parties' understand that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to 'The Parties' information systems **must**:

- Be suitable for their roles.
- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information relevant to the jobholders' role and duties.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any user's access to information or information systems used to deliver 'The Parties' business.

Access to 'The Parties' information systems will not be permitted until the requirements of this policy have been met.

4. Roles and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the Information Asset Owner – please refer to Information Protection Policy (see Appendix 7).

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the Joint ICT Service in a timely manner, using an agreed process.

The information security responsibilities of every user include familiarisation with the Information Security Policy and its Appendices, and the signing of a statement confirming that the user is aware of, and understands, these policies. (See Appendix 13)

4.1 User Screening

Background verification checks are carried out on all employees by HR, please see the HR recruitment and selection policy for details.

ICT staff with network administration rights and, where appropriate or required by 3rd party agreements, will also require standard checks through the Disclosure and Barring Service.

Where access is to systems processing payment card data, credit checks on the user must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

4.2 Management Responsibilities

Line managers must notify ICT in a timely manner of any changes in a user's role or business environment, to ensure that the user access can be changed as appropriate. Processes must ensure that access to information systems is extended to include new user requirements and that any access that is no longer needed is removed.

Any changes to a user's access must be made in a timely manner and be clearly communicated to the user.

Service managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate 'The Parties' policies. These policies include:

- Information Protection Policy (Appendix 6)
- Information Security Incident Management Policy (Appendix 11)

This requirement must be documented.

4.3 Information Security Awareness, Education and Training

All users of ICT systems are required to undertake security awareness training and should take note of updates in related statute and organisational policies and procedures as relevant for their role.

It is the role of Service managers to ensure that their users are adequately trained and equipped to carry out their role efficiently and securely.

5. Applying the Policy – When Access to Information or Information Systems is No Longer Required

5.1 Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to 'The Parties' information assets is removed in a timely manner when no longer required by the user.

5.2 Return of Assets

Users must return all the organisation's assets, for example, laptops, tablets, mobile phones and memory sticks in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

APPENDIX 6 - INFORMATION PROTECTION POLICY

1. Introduction

Information is a major asset that 'The Parties' have a responsibility and requirement to protect. Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that 'The Parties' maintain. It also covers the people that use them, the processes they follow, and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, integrity, and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at 'The Parties' . The policy specifies the means of information handling and transfer within 'The Parties' .

2. Scope

The policy applies automatically to all the systems, people and business processes that make up 'The Parties' information systems.

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who have access to Information systems or information used for 'The Parties' purposes.

3. Principles

'The Parties' will ensure the protection of all information assets within the custody of 'The Parties'.

High standards of confidentiality, integrity and availability of information will be always maintained.

This policy should be applied whenever 'The Parties' Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape, DVD or video.
- Speech.

4. Applying the Policy

4.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders (Cloud based or on premise).
- Software licenses.
- Physical assets (computer equipment and accessories, mobile devices, removable media).

- Key services.
- Key people.
- Intangible assets such as reputation and brand.

'The Parties' must draw up and maintain inventories of all important personal data assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management, and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

4.2 Data Retention

'The Parties' have data retention policies in place.

4.3 Personal data

Personal data is any information about any living, identifiable individual. This could be customer, employee, or member personal data. 'The Parties' are legally responsible for it. Its storage, protection and use are governed by current data protection legislation. Details of specific requirements can be found in the Legal Responsibilities Policy.

4.4 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

4.5 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

4.6 Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by users. All users must be informed of their responsibility for the documents they create.

4.7 Corporate Information Assets

For information assets whose use throughout 'The Parties' is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated, and the responsibility clearly documented. This should be the person who has the most control over the information.

4.8 Information Storage

All electronic information will be stored on pre-determined centralised facilities (hosted on premise or in the Cloud) to allow regular backups to take place.

Users are not allowed to access information until a line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
Databases holding personal information have a defined security and system management procedure for the records and documentation.
This documentation will include a clear statement as to the use, or planned use of the personal information.
Files which are identified as a potential security risk should only be stored on secure network areas.

5. Disclosure of Information

5.1 Sharing OFFICIAL-SENSITIVE Information with other Organisations.

OFFICIAL-SENSITIVE information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.
An official email legal disclaimer must be contained with any email sent. This can be found in the Email Policy.
The disclosure of OFFICIAL-SENSITIVE information in any way other than via secure email is a disciplinary offence. If there is suspicion of a user treating OFFICIAL-SENSITIVE information in a way that could be harmful to 'The Parties' or to the data subject, then it is be reported to the internal audit section, and the person may be subject to disciplinary procedure.
Any sharing or transfer of 'The Parties' information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular, this must be compliant with current data protection legislation, The Human Rights Act 2000 and the Common Law of Confidentiality.

APPENDIX 7 - COMPUTER, TELEPHONE AND DESK USE POLICY

1. Introduction

'The Parties' rely on the widespread use of technology and ICT facilities to maintain business both in the offices and at remote locations.
As such, there is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for the pursuance of personal interests or for amusement/entertainment.
'The Parties' also handle large amounts of OFFICIAL-SENSITIVE information. The security of this information is of paramount importance. Working towards a clear desk policy can help prevent the security of this information from being breached.
The purpose of this document is to establish guidelines as to what constitutes "computer and telephony resources", what is considered to be "misuse" and how users should work towards a clear desk environment.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees 'The Parties', contractual third parties and agents, work experience and volunteers who have access to information systems or information used for 'The Parties' purposes.

3. Principles

This policy should be applied whenever users who access information systems or information utilise 'The Parties' computer and telephony resources.
Computer and telephony resources include, but are not restricted to, the following:

- Centralised server and storage systems
- Hosted solutions (Cloud/SaaS)
- Personal computers.
- Portable laptop computers.
- Removable media (memory cards and sticks)
- Mobile devices (smart phones, tablets)
- Printers.
- Network equipment.
- Telecommunications facilities.

4. Computer Resources Misuse

No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case will need to be considered. However, some examples are outlined below:

- Use of computer resources for the purposes of fraud, theft, or dishonesty.
- Storing/loading/executing of software for a purpose which is not work related.
- Storing/loading/executing of software:
    - which has not been acquired through approved procurement procedures, or
    - for which 'The Parties' does not hold a valid program licence, or
    - which has not been the subject of formal virus and security checking procedures.
- Storing/processing/printing of data for a purpose which is not work related.

For further information, users are requested particularly to read the following policies:

- Email Policy (Appendix 1)
- Internet Acceptable Use Policy (Appendix 2)
- Software Policy (Appendix 3)

5. Clear Desk

'The Parties' would wish to ensure that all information is always held securely. Ideally, work should not be left on desks unattended and should be removed from view when unsupervised.

At the end of each day desks should, wherever possible, be cleared of all documents that contain any protectively marked documents as per the classification scheme of the Council or data owner or any information relating to staff, clients, or customers. This information must be stored in a facility (e.g., lockable safe or cabinet) commensurate with this classification level. If employees find this difficult because of accommodation issues, the matter should be raised with their Line Manager in the first instance.

Unclassified material or publicly available information may be left tidily on desks. A definition of the Government marking schemes can be found in the ICT Policy Summary Document.

Documents should not be left lying on printers, photocopiers, or fax machines.

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

Computer screens must be locked to prevent unauthorised access when unattended and screens should lock automatically after a period of inactivity, in order to protect information. A screen saver with password protection enabled must be used on all devices. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action. The screen saver should be the one supplied by IT, no personal screen savers are to be used.

Users of hot desk stations must ensure that it is left in the state in which it was found. Remember, when you are not working at your workstation there could be a business requirement for other users to use that station.

APPENDIX 8 - REMOTE WORKING

1. Introduction

'The Parties' provide portable computing devices to assist users to conduct official business efficiently and effectively from remote sites including home working. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets, and safeguarded appropriately.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who use 'The Parties' IT facilities and equipment when working on official business away from the organisation (i.e. working remotely), or who require remote access to 'The Parties' information Systems or information.

3. Principles

'The Parties' information systems or information must not be accessed whilst outside the United Kingdom regardless of who owns the IT equipment, without agreement of the Joint ICT Service and in line with the current National Cyber Security Centre or UK Government guidelines.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Smartphones
- Tablets
- Mobile phones.
- Wireless technologies.

4. Applying the Policy

All IT equipment (including portable computer devices) purchased for users by 'The Parties' is the property of the purchasing authority. It must be returned upon the request of the purchaser. All IT equipment will be supplied and installed by Joint ICT Service staff. Hardware and software **must only** be provided by the purchasing authority via the ICT team.

Access to 'The Parties' systems and data is restricted to corporately managed and owned ICT equipment.

5. User Responsibility

It is the user's responsibility to ensure that the following points are always adhered to:

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users will not install or update any software on to 'The Parties' owned portable computer device.
- Users will not install any screen savers on to 'The Parties' portable computer device.
- Users will not change the configuration of 'The Parties' owned portable computer device.
- Users will not install any hardware to or inside any 'The Parties' owned portable computer device, unless authorised by the Joint ICT department.

- Users will allow the installation and maintenance of 'The Parties' installed Anti-Virus updates immediately.
- Users will inform the Joint ICT Service of any 'The Parties' owned portable computer device message relating to configuration changes.
- Business data should be stored in 'The Parties' approved, hosted or cloud solutions and not be stored permanently on the portable computer device.
- All faults must be reported to the Joint ICT Service.
- Users must not remove or deface any asset registration number.
- Users registration must be requested from the Joint ICT Service. Users must state which applications they require access to.
- Users requests for upgrades of hardware or software must be approved by a line manager. Equipment and software will then be purchased and installed by the Joint ICT Services.
- The IT equipment can be used for personal use by users so long as it is not used in relation to an external business and does not conflict with 'The Parties' business or policies. Only software supplied and approved by the Joint ICT Service can be used (e.g. Word, Excel, Adobe, etc.).
- No family members may use the ICT equipment. The ICT equipment is supplied for the user's sole use.
- Take care when using mobile devices in public areas, access your surroundings to protect from people looking over your shoulder, listening into conversations, near CCTV coverage.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, 'The Parties' may recover the costs of repair.
- The user must not take any of 'The Parties' equipment outside the United Kingdom as the equipment may not be covered by 'The Parties' normal insurance and it is liable to be confiscated by airport security personnel.
- 'The Parties' may at any time, and without notice, request software and hardware audits, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database or carry out any processing of OFFICIAL-SENSITIVE information relating to 'The Parties'. **Under no circumstances** should personal or security marked information be emailed to a private non 'The Parties' email address or uploaded to a non 'The Parties' storage area. For further information, please refer to the Email Policy.
- Any data transferred from 'The Parties' systems must only be undertaken using a corporate provided encrypted memory stick.
- Any users accessing PSN services or facilities, or using OFFICIAL-SENSITIVE information, must only use 'The Parties' owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely.
- Equipment must not be left unattended in public places and must not be left visible in a vehicle.
- Laptops should be carried as hand luggage when travelling.
- Any loss of equipment should be reported immediately to the ICT Service Desk and, if appropriate, to the Data Protection Officer.

6. Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. Equipment must be secured whenever it is not in use.

No removable media devices or paper documentation should be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people, and the onus is on the employee to maintain confidentiality. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. All documents classified as OFFICIAL-SENSITIVE must be disposed of via confidential waste facilities.

Always use portable equipment in accordance with other legislation, for example when using a mobile phone whilst driving you must comply with current legislation and other Council policies.

7. Access Controls

It is essential that access to all OFFICIAL-SENSITIVE information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or user login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL-SENSITIVE data held on the portable device must be encrypted. Personal data can only be stored on encrypted devices. It is ICTs responsibility to provide encrypted devices and the employees to ensure they are used.

Only methods approved and provided by the Joint ICT Service must be configured to allow remote access to 'The Parties' systems if connecting over Public Networks, such as the Internet.

Multi-factor authentication must be used when accessing 'The Parties' information systems remotely and access must only be via corporately owned equipment.

8. Anti-Virus Protection

All Council devices have antivirus protection. Under no circumstances should this be disabled or modified.

If there is an error or warning showing on the anti-virus, you should contact the Joint ICT ServiceDesk to report the issue.

You must, assist the Joint ICT ServiceDesk to take your device into the office to update the anti-virus or Operating updates when asked to do so.

9. Users Awareness

All users must comply with appropriate codes and policies associated with the use of IT equipment as contained within the Information Security Policy and its appendices.

All users must complete mandatory Security Awareness Training and Data Protection training.

It is the user's responsibility to ensure their awareness of and compliance with these.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to OFFICIAL-SENSITIVE information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as 'The Parties' are.

APPENDIX 9 - REMOVABLE MEDIA POLICY

1. Introduction

This policy establishes the principles and working practices that are to be adopted by all users for data to be safely stored and transferred on removable media.
This policy aims to ensure that the use of removable media devices is controlled to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of 'The Parties' computer network.
- Avoid contravention of any legislation, policies, or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

A definition of the national protective marking scheme and government security classifications can be found in the PSN acceptable usage policy (see appendix 5).

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, 'The Parties' , contractual third parties and agents, work experience and volunteers who have access to 'The Parties' information systems or IT equipment and intends to store any information on removable media devices.

3. Principles

'The Parties' will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official 'The Parties' business.
Removable media devices include, but are not restricted to the following;

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP4 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines)
- Video tapes

4. Risks

'The Parties' recognise that there are risks associated with users accessing and handling information to conduct official 'The Parties' business. Information is used throughout 'The Parties' and sometimes shared with external organisations and applicants. Securing OFFICIAL-SENSITIVE data is of paramount importance – particularly in relation to the council's need to protect data in line with the requirements of the General Data

Protection Regulations 2018. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of 'The Parties'. It is therefore essential for the continued operation of 'The Parties' that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to 'The Parties' needs.

5. Restricted Access to Removable Media

It is 'The Parties' policy to prohibit the use of all removable media devices without approval. The use of removable media devices will only be approved if a valid business case for its use is developed. There are significant risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the IT Section. Approval for their use must be given by a Service Manager or Senior Manager, this should be done via a request to the service desk. This applies to the devices themselves, including memory sticks but not the media such as CD's, DVD's and audio and video tapes.

If memory sticks are found in the office or outside, these should **not** be inserted into Council equipment as they may contain malicious files. These should be handed into the Servicedesk.

Should access to, and use of, removable media devices be approved the following sections apply and must be always adhered to.

6. Procurement of Removable Media

All removable media devices, including memory sticks, and any associated equipment and software must only be purchased and installed by ICT Services. Procurement of consumable media such as CD's, DVD's and audio and visual may be procured through standard procurement channels. Non 'The Parties' owned removable media devices and media **must not** be used to store any information used to conduct official 'The Parties' business and **must not** be used with any 'The Parties' owned or leased IT equipment. The only equipment and media that should be used to connect to 'The Parties' equipment or 'The Parties' network is equipment and media that has been purchased by 'The Parties' and approved by the Joint ICT Service or has been sanctioned for use by ICT Management.

7. Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction, or malfunction of equipment than data which is frequently backed up. Therefore, removable media should not be the only place where data obtained for 'The Parties' purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system. For further information please see the Remote Working Policy (see Appendix 9).

To minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL-SENSITIVE data, personal or sensitive data held must be encrypted.

Users should be aware that 'The Parties' will audit / log the transfer of data files to and from all removable media devices and 'The Parties' owned IT equipment.

8. Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the Joint ICT Service who will access the breach to determine the appropriate course of action. The Data Protection Officer should also be informed where appropriate.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to ICT Management as referenced in the Information Security Incident Management Policy (see Appendix 10).

9. Third Party Access to 'The Parties' Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from 'The Parties' network, information stores or IT equipment without explicit agreement from the Joint ICT Service Management and the Data Protection Officer.

Should third parties be allowed access to 'The Parties' information then all the considerations of this policy apply to their storing and transferring of the data.

10. Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the Joint ICT Service should removable media be damaged and return to ICT for secure disposal.

Virus and malware checking software approved by the Joint ICT Service must be operational on any device managed and owned by 'The Parties' . It is the user's responsibility to ensure appropriate and up to date virus and malware software is operational on any non 'The Parties' device that the removable media device is connected to or seek assurances to that effect.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to 'The Parties', other organisations or individuals from the data being lost whilst in transit or storage.

11. Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within 'The Parties' or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. **All removable media devices that are no longer required, or have become damaged, must be returned to the Joint ICT Service for secure disposal**.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the Joint ICT Service.

12. Users Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices.

13. Specific guidance for laptop and tablet users

- Laptops and tablets should remain with staff when they leave the office, this supports business continuity in the event of adverse weather and any issues with access to office buildings.
- If a laptop or tablet must be left in the office overnight or at weekends these should be placed out of sight preferably in a locked drawer or cupboard.
- Laptops and tablets should not be left on display in a car such that it would encourage an opportunist theft.
- If travelling by public transport it may be advisable to use a bag that may be less identifiable as a laptop or tablet case.

APPENDIX 10 - INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

1. Introduction

This policy needs to be applied as soon as information systems or data are suspected to be or are affected by an adverse event which is likely to lead to a security incident.
The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.
An information security incident includes, but is not restricted to, the following:

- The loss or theft or corruption of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees 'The Parties', contractual third parties and agents, work experience and volunteers who have access to 'The Parties' information systems or IT equipment.
All users **must** understand and adopt use of this policy and are responsible for ensuring the safety and security of 'The Parties' systems and the information that they use or manipulate.
All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.
Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious

- Malicious code: Malware, virus or ransomware.
- Phishing: Emails, Texts, or phone calls attempting to convince someone to trust a link or attachment or to action something malicious to give them access to council data or to infect council devices.
- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.

- Cloud based: attack on cloud-based applications.
- Being notified of a third-party security breach.

Misuse

- Use of unapproved or unlicensed software on 'The Parties' equipment.
- Accessing a computer database using someone else's authorisation (e.g., someone else's user id and password).
- Sharing usernames and passwords.
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.
- Sending a sensitive e-mail to 'all staff' by mistake or to the wrong recipient.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any 'The Parties' computer equipment.
- Theft / loss of data via third-party supplier.

4. Procedure for Incident handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Joint ICT Service to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the Joint ICT Service to gain as much information as possible from the business users to identify if an incident is occurring.

The following sections detail how users must report information security events or weaknesses.

4.1 Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand and be able to identify that any unexpected or unusual behaviour on the device could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from ICT support staff.
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the ICT Service Desk on ext. 3001 or external number 01246 217103.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported immediately to senior management and the Data Protection Officer for the impact to be assessed.

The Joint ICT Service will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of the person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

The Data Protection Officer will require:

- A contact name and number of the person reporting the incident.
- Type of data
- Details of steps already taken

4.2 Reporting a suspected phishing attempt.

If you are unsure whether an email, weblink or attachment is legitimate you should contact the Servicedesk for advice. If you have clicked on an email, link, opened an attachment or entered credentials and it doesn't seem right, contact the Servicedesk for advice, to help remedy the situation and prevent it impacting others.

4.3 Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered as misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to the Joint ICT Service. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by the Joint ICT Service.

4.4 Collection of Evidence

If an incident may require information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact the Joint ICT Service for advice.

The actions required to recover from the security incident must be under formal control. Only identified and authorised users should have access to the affected systems during the incident, and all the remedial actions should be documented in as much detail as possible.

The officer responsible for an incident should risk assess the incident based on the Corporate Risk Impact Methodology.

APPENDIX 11 - IT INFRASTRUCTURE SECURITY POLICY

1. Introduction

The purpose of this policy is to establish standards regarding the physical and environmental security of 'The Parties' information. Personal, confidential and protectively marked information (see Glossary) that 'The Parties' holds and uses, and to comply with legislative requirements, information security best practice, and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Public Services Network(PSN), access to 'The Parties' information equipment and information must be protected.

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect 'The Parties' IT data centre. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. No service should fall below the baseline security standard level of protection required for their teams and locations.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all departments, partners, employees of 'The Parties', contractual third parties and agents, work experience and volunteers who have access 'The Parties' equipment and information (electronic and paper records). They are responsible for ensuring the safety and security of 'The Parties' equipment and the information that they use or manipulate.

3. Principles

There shall be no unauthorised access to either physical or electronic information within the custody of 'The Parties'.
Protection shall be afforded to:

- IT equipment that holds Electronic data
- IT equipment used to access electronic data.
- IT equipment used to access 'The Parties' network.

This policy applies to all users of 'The Parties' owned or leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to 'The Parties' should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles, and the contribution users make to the safe and secure use of information within the custody of 'The Parties'.

This policy should be applied whenever a user accesses 'The Parties' information equipment. This policy applies to all locations where information within the custody of 'The Parties' or information processing equipment is stored, including remote sites.

4. Secure Areas

OFFICIAL- SENSITIVE information **must** be stored securely. A risk assessment should identify the **appropriate** level of protection to be implemented to secure the information being stored.
Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised, they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g., fire, flood, vandalism.

Access to secure areas such as the data centre and ICT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Users working in secure areas should challenge anyone not wearing a staff or visitor badge. Each Service must ensure that doors and windows are properly secured at the end of each working day.
Identification and access tools/passes (e.g., badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.
Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A council ICT employee must monitor all visitors accessing secure ICT areas at all times.
Keys to all secure areas housing ICT equipment and lockable ICT cabinets are held centrally by the ICT Service, as appropriate. Keys are not stored near these secure areas or lockable cabinets.
In all cases where security processes are in place, instructions must be issued to address the event of a security breach.

If a user leaves outside normal termination circumstances, all identification and access tools/passes (e.g., badges, keys etc.) should be recovered from the users and any door/access codes should be changed immediately.
Please also refer to the ICT Access Policy and Human Resources Information Security Standards.

6. 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.
- If laptops or tablets must be left at the office overnight then they should be kept out of sight, preferably in a locked drawer or cabinet.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs and laptops should not have data stored on the local hard drive. Data should be stored either on network file servers, within corporate applications or systems 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 ICT Services.
All items of equipment must be recorded on an inventory, maintained by ICT. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.
All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the ICT inventory.
For portable computer devices please refer to the Remote Working Policy (appendix 9).

7. 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, Health and Safety guidance should be sought if in any doubt.

8. Security of Equipment off Premises

Please refer to the Remote Working Policy.

9. Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must be returned to the Joint ICT Service for data removal.

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

Appendix 12 – WHATSAPP POLICY

10.1 Introduction

WhatsApp is becoming an increasingly popular mobile application, a large proportion of the population now use the application to message, call and share files and photographs with their friends and family.

This protocol only covers the use of WhatsApp for 'The Parties' purposes.

Officers may choose to use WhatsApp to communicate with each other in a social context using non corporate devices. Employees who use WhatsApp in a social context on personal devices must **not** share or discuss matters which contain commercially sensitive or personal data belonging to 'The Parties'. Employees who discuss or share this information in a social context may be in breach of the terms of employment contract and could face disciplinary action.

Under the UK General Data Protection Regulation and the Data Protection Act 2018 the Council must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This means that we must have in place appropriate security measures to ensure that personal data held by the Councils (Data Controllers) is stored and transferred securely, especially when using third party processors and applications such as WhatsApp.

Employees can now use Microsoft Teams on Council provided devices instead of WhatsApp to share files, photos and collectively collaborate. Microsoft Teams is the Council's Corporately preferred collaboration tool.

However, employees may request to have WhatsApp installed on their council issued devices subject to advice from ICT and the Data Protection Officer and approval from Senior Manager for the Service for the following Council purposes of business continuity.

10.2 Business Continuity

WhatsApp can be used as a communication tool within teams to aid business continuity.

Some employees have designated responsibilities for business continuity and as such will have WhatsApp on their council phone for this purpose.

Other employees and teams may wish to have a WhatsApp group for this purpose on their personal phones. Communicating with work colleagues using WhatsApp assumes that they are comfortable with downloading and

corresponding via the app. The app requires access to your phone contacts when setting up and these are stored on the WhatsApp server. As such employees have a choice over its use. Managers will need to consider contact arrangements for those colleagues who do not wish to use WhatsApp such as direct contact by phone.

Potential uses include:

- Providing information on office closures, urgent Council updates to employees who do not have access to e-mail.
- Informing colleagues and managers that you are unable to attend the office due to adverse weather.
- Arranging shifts etc, with casual staff workers who do not have access to other corporate communication.

A limited amount of personal data is involved in using WhatsApp for this purpose, specifically the name and phone number of the individuals within the group.

These WhatsApp groups should only be used for business continuity purposes and should not contain any sensitive data. Discussions on council issues or workload should be conducted by phone, in 1 to 1's or team meetings and email.

It is the responsibility of the user to ensure that the group membership on WhatsApp is kept up to date and the information is shared to the correct recipients.

10.3 Reasons for this approach

The Councils have taken a strict approach to protect themselves and their employees.

Unlike Microsoft Teams, Emails etc, WhatsApp is not a corporately managed tool and chats by their nature cannot form part of 'The Parties' official records. They live on the device and are accessible by the sender and the receiver. This has the following risks:

- Reduces transparency in public tasks.
- Restricts accessibility to council records.
- Complicates requests for information under access legislation e.g., FOIA, subject access under GDPR.
- Could make employees susceptible to bullying and harassment.
- Could pose a safeguarding risk.
- Inappropriate and/or unlawful sharing of personal data (a data breach)
- Loss of control over WhatsApp group management e.g., not removing group members who no longer need access.

- Impacts on the Councils' ability to undertake investigations, review decisions etc.
- Difficulty confirming the integrity of the sender / recipient.

Unfortunately, there are numerous cases where employees of other organisations, have unlawfully shared their organisation's personal data via WhatsApp and other messaging services which has led to their dismissal.

Information that is unlawfully shared amounts to a 'personal data' breach. If the breach is severe enough the Councils could be liable to be fined by the Information Commissioner's Office (ICO). The UK's independent regulator set up to uphold data rights for individuals.

10.4 Tips on using WhatsApp safely on a council device if authorised to do so.

- Apply the same etiquette to WhatsApp messages as you would apply to any other work correspondence: Remain professional; use neutral, professional language and tone.
- Do not share personal/confidential information over WhatsApp.
- The chat does not replace the formal council record. Keep separate records in the appropriate council system.
- Remember that WhatsApp chats may be subject to freedom of information (FOI) requests or subject access requests (SARs).
- Take care to ensure that the content of the chat cannot be interpreted as harassment, discrimination, or abuse.
- Report any chats that you receive which are inappropriate e.g., abusive, discriminatory etc.
- Do not allow anyone else to use your corporate device.
- Disable message notifications on your device's lock-screen.
- Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your address book.
- If you are a group administrator, take great care when selecting the membership of the group, and review the membership regularly.
- You may want to unlink the app from your photo library.
- This protocol should be used in conjunction with the Mobile device Policy and Information and Cyber Security Policy.
- Be aware of Phishing / Scams, ensure the message is from who you think it is.

10.5 FAQ's

10.5.1 How do I request the use of WhatsApp on a Council device?

You should first discuss the need to use WhatsApp with your line manager. If your line manager agrees that use of WhatsApp is necessary, they should contact the Councils' Data Protection Officer (DPO) and ICT using the contact details below:

DPO: Kath Drury – kath.drury@bolsover.gov.uk 01246 242280

IT: servicedesk@ne-derbyshire.gov.uk

10.5.2 My manager has asked to add me to a business continuity WhatsApp, but I am not comfortable with team members having access to my personal phone number, what can I do?

In the first instance you should discuss your concerns with your line manager and make alternative arrangements.

You might be able to come to a more suitable arrangement where you and your line manager contact each other directly.

10.5.3 Can information sent over WhatsApp be requested by members of the public under the Data Protection (DPA) and Freedom of Information Act (FOIA)?

Yes, if WhatsApp is being used for council purposes, then information on it could fall within scope of a request made under the DPA and FOIA as the Councils would be the data controllers and applicable authorities respectively. As such all the relevant customer service standards and policies apply to employees using this mobile application as other method of contact for council business.

10.5.4 What security features does WhatsApp have?

The following are some of WhatsApp's security features (including links to tips on strengthening the security):

10.5.5 WhatsApp and consent

saying 'OK' to allowing access to your phone contacts when setting up the app will upload the numbers of all your contacts to the WhatsApp servers (in the US or Ireland). All chat content is shared with the group and/or individual selected and stored on your phone and theirs. Chats can be exported and forwarded. Dependant on your settings, your photo and online status may be visible.

10.5.6 Data Portability

You can request your own account information from WhatsApp, but this does not include your message history.

10.5.7 Account Deletion

You can delete your account information and profile photo. Deleting your account will remove you from all groups, delete undelivered messages and delete the message history held on the phone and in an iCloud or Google drive backup (if set).

10.5.8 End-to-end Encryption

Applies to messages in transit and is set to on by default. Encryption ensures that only the sender and the recipient can read the message whilst in transit. Third parties can't and neither can WhatsApp. Work mobiles are encrypted, and pin protected to protect the data whilst it is on the phone. If you lose you work phone, ensure you report it to ICT so they can send out a remote wipe request.

10.5.9 Deletion of messages

Delivered messages are automatically deleted from WhatsApp's servers, including chats, photos, videos, voice messages, files and location information shared with your contacts. Messages, however, will be retained in a backup (iCloud or Google drive) if you have set this. Chats are retained on the WhatsApp servers until they can be delivered; if a message is on the WhatsApp servers for more than 30 days it is deleted.

10.5.10 Inactive accounts

Any account which is inactive for 120 days is deleted.

10.5.11 Restriction on forwarding chats

When you forward a message, you can share it with up to five chats at one time. However, when a message is forwarded through a chain of 5 or more chats (meaning it's at least 5 forwards away from its original sender) the message is labelled with a double arrow icon. These messages can only be forwarded one chat at a time, to help keep conversations on WhatsApp more private and personal.

10.5.12 Sending photos

Whilst there isn't any functionality in WhatsApp to stop users sending photos, it is possible to make sure that photos aren't automatically saved to your phone's photo gallery. To change the settings so that images are not saved, follow the guidance here. Changing the settings will also help to reduce the amount of storage that is used by WhatsApp.

Further details on controlling your privacy including managing your profile photo, group privacy settings and status updates, can be found here.

11 APPENDIX 13 – MICROSOFT TEAMS POLICY

11.1 Introduction

The authority accepts the use of Microsoft Teams is essential to enabling the authority to meet its aims and objectives. It is a requirement that use of this software by all employees is legal and appropriate for delivering the authorities responsibilities and does not create unnecessary risk.

Microsoft Teams enables you and your colleagues to send instant messages, make video and audio calls, share, and edit files as a team and with external partners where appropriate.

Some of the functionality of Teams has been limited whilst the authority ensures that the correct security and user training is in place to reduce the risks to the authority's data and systems. This is a corporate communication tool for use within the workplace and for work related activities. Additional functionality will be added over time and consequently, these protocols and procedures will be regularly updated and redistributed.

This policy should apply to all users who have access to the authorities ICT facilities and should be read in conjunction with current policies.

11.2 Best Practice

11.2.1 Chats

- Microsoft Teams supports storing of sensitive information up to UK classified status. However, you need to be very careful when sharing any sensitive data that you know who you are sharing this with, especially when sharing to a Team or during a meeting. You should not share sensitive personal information through Team chat. When referring to individuals try to avoid giving personal information which clearly identifies an individual. Be particularly careful with sensitive personal data e.g., health information, banking details etc. Is it possible to discuss individual scenarios or refer to cases using a de-personalised reference if necessary. It is important to ensure that the individuals cannot be identified from the information being discussed by anyone not authorised to know.
- When sharing information, you should always check the membership of the Team or Channel you are collaborating with. Be aware that Team Owners can change the members of a Team and access to information in previous chats would be available to them. Chats from Team meetings may be retained.

- You can get a colleague's attention by using @ and their name into the chat.
- All chat must comply with Customer Services Standards and people must be treated with respect, dignity, and courtesy. Communications should be professional, and in line with workplace expectations. Team chats are auditable.
- Under no circumstances should users communicate material which is, for example defamatory, obscene, or does not comply with the Authority's Equalities Policy (HR) and Equality & Diversity Policy for Service Delivery, or which could be anticipated to be considered inappropriate. Bullying and harassment is not tolerated at the Council and this corporate system should not be used for that purpose.
- Emojis and GIFs are currently enabled on Teams, only use these when it is appropriate to do so. Emojis and GIFs may mean different things to individuals and can easily be mis-interpreted. Be especially careful when using these to communicate and if in doubt, use an alternative communication method to get your point across.
- You should always use your Council provided Teams logon to access Council related Teams content and this logon should only be used for Council related purposes.
-

11.2.2 Meetings and Calls

- Microsoft Teams is the authority's approved software for video/audio conferencing.
- It is possible to voice or video call people internally using Teams.
- It is not possible to call external phone numbers using Teams, you will need to use the authorities current phone system to do this.
- Double check you have sent any meeting invites to the correct attendees.
- Be careful when entering information in chats sent during meetings as they are visible to everyone invited to the meeting and can be accessed after the meeting has ended.
- Everyone provided with a corporate email address and access to Teams, will be licenced to use Microsoft Teams to arrange meetings without reduced time or participant limitations.
- Think about what people can see in the background, consider using the blur or selecting a corporately approved background picture. Your authority will have provided some authority specific backgrounds for your use.
- Think about what people can hear, especially when working from remote locations. Mute your microphone when not speaking and

consider using a headset as many of these are noise cancelling and could prevent conversations being over heard.

- Whilst on video calls wear appropriate clothing in line with your authority's corporate guidance.
- Before screen sharing, ensure data which shouldn't be shared is not visible on the screen.
- Do not allow others outside of the authority control of your keyboard or mouse.
- Team meetings can be used to share files and links; it is your responsibility to ensure any files are shared appropriately and with the correct participants.
- Be vigilant about downloading unknown files as these could be malicious or contain viruses.
- Teams will create a link and a meeting id and password. To prevent uninvited attendees to your meeting be careful who you share these details with.
- Trusted Authority members (who are logged on with a corporate account) will automatically be allowed into a meeting room, however those external to the trusted authorities are put into a Lobby (waiting room) until the host lets them in.
- Meetings are not to be recorded unless there is a legitimate reason for doing so. If this is the case advise the participants at the beginning of the meeting, advise them of the purpose of the recording, who it will be shared with and how long, it will be retained for. The recording of the meeting will be stored in the host's OneDrive. Recordings will be automatically deleted after 60 days. You will be responsible for deleting the recording if the agreed retention has expired. You should not record meetings that include customer data, Official-Sensitive data, or personal staff information. Recordings and transcriptions must be deleted if they contain any personal /sensitive data.
- Teams will automatically transcribe recorded meetings, or meetings where transcription is enabled. The meeting host should inform participants that the meeting is being transcribed and provide the purpose of the transcription, who it will be shared with and for how long. Transcripts will be automatically deleted after 60 days.

11.2.3 Roles and Responsibilities

There are three roles within M365 for a Team: Teams ICT Administrators, Teams Owners, and Team Members. Most users of a Teams site will be members.

11.2.4 Teams ICT Administrators

New Teams can only be created by ICT. ICT can add and remove users to specific Teams and designate Team Owners. Each Team must be assigned a minimum of two Team/Site Owners. ICT cannot see the content of chats they are not a member of unless they have been asked to retrieve information.

11.2.5 Teams/Site Owners (Administrative and Accountable)

Site Owners are accountable for ensuring that any of their information assets or extracts from those assets are managed appropriately within Microsoft Teams in line with their responsibilities.
Teams Site Owners are responsible for:

- Creating and deleting Teams Channels when necessary.
- Ensuring there are sufficient active Teams/Site Owners for a specific Teams site (minimum of 2)
- Adding and removing Team members and owners.
- Ensuring that the user of information on the Teams site is compliant with the Acceptable Use Policies.
- Ensuring that chats within Teams Channels are used in an appropriate manner and follow council policies on appropriate behaviour.

11.2.6 All Staff (Teams Site Members)

All staff are responsible for:

- Their own activity within Teams
- Ensuring that the use of information on the Teams site is compliant with the ICT Security Policy, including the Acceptable use policy and General Data Protection and Retention policies and any other relevant policies.
- Ensuring that chats within Teams Channels are used in an appropriate manner and follow council policies on appropriate behaviour.

11.2.7 Recovery

Teams is a collaboration tool for temporary time sensitive discussions. Although Microsoft have processes in place to recover the details and it is unlikely data would be lost, we cannot guarantee that data can be restored if deleted or corrupted.
Therefore, it is important that data or files which you need to retain should have original copies retained either on the authorities file drives or in designated department systems (e.g., S drive or X drive, Uniform,

Corporate DMS etc). This ensures that the Authorities can rely on their records for business and legal purposes.

11.3 Retention and Monitoring

11.3.1 Monitoring

- All users should be aware that all Teams usage is monitored and recorded centrally. Whilst respecting the privacy of authorised users, the authority maintains its legal right, in accordance with the Regulation of Investigatory Powers Art 2000, to monitor and audit the use of Teams content by authorised users to ensure adherence to this policy. Any interception or monitoring will be carried out in accordance with the provisions of that act.
- The authority reserves the right, with written approval from an appropriate Director or Assistant Director or the Human Resources & OD Manager, to monitor chats and information sent within the authorities Teams system and to access this data without notifying the individual concerned that the right is being exercised.
- Please note inappropriate use of the system could result in disciplinary action being taken.

11.3.2 Retention

Chat content, whether direct or within channels is searchable and could therefore be disclosable under freedom of information (FOI) or subject access requests (SAR). Both are applicable to information held by the Council in a recorded form. It is therefore important that data is not kept beyond its requirement and is compliant with GDPR.

- One to one and one-off group chats are retained for 3 months before being deleted.
- Individual Teams are retained for 12 months after last use. At that point the Team Site Owner will be contacted and asked whether there is any business need for the Team to be kept for longer, otherwise the Team will be deleted.
- Team Channel chats will be kept for 12 months after last use.

11.4 Accessing Microsoft Teams

- Microsoft Teams can only be accessed by corporately managed devices such as works Laptops, Virtual desktops, mobile phones, or tablet devices such as iPads.
- You should not log onto Microsoft Teams on any other devices except corporately managed work devices provided by the authority.

- The Teams app will be automatically installed on all corporate laptops and virtual desktops.
- The Teams app will be made available on all corporately managed Mobile phones and iPads, providing they are used by a licenced user of M365 and have been enrolled on the Microsoft Endpoint Manager / Intune (MEM)
- You can also access Teams via a web browser from a corporately managed device https://teams.microsoft.com/
- Teams should only be used for Council related activities.
- You should only log onto Teams using your corporately assigned logon which is usually your email address and network password.
- Be aware of Phishing scams which may ask you to click dubious links or ask you to enter your credentials.
- Audio/Video conferencing tools provide another way to communicate. If you are struggling to hear the conference or having difficulties with the software, please discuss this with your line manager.

11.5 Microsoft File Sharing

- Teams and OneDrive provides the ability to share files with other members of the Team.
- You are responsible for ensuring that files are only shared to the appropriate people within the team.
- Files should have the appropriate protective marking applied (official or official-sensitive).
- You are responsible for removing files once they are no longer needed and in line with the records, retention, and disposal schedules.
- We cannot guarantee that files stored on Teams file stores can be retrieved, so always retain a copy of any files on the authorities file drives or in designated department systems (e.g., S drive or X drive, Uniform, Corporate DMS etc).

Appendix 14 GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

11.6 Purpose

The purpose of this policy document is to provide a framework for the use of Generative Artificial Intelligence Large Language Model tools (collectively referred to in the rest of this document as GenAI) such as ChatGPT, Bard, Bing or other similar tools by 'The Parties'.
This policy is designed to ensure that the use of GenAI is ethical, complies with all applicable laws, regulations, and council policies.
The pace of development and application of GenAI is such that this policy will be in a constant state of development.
Generative artificial intelligence (GenAI) can create realistic, human-like text, images, code and art based on huge amounts of (usually public) data it has been trained on. It can produce a range of useful outputs, like text, audio, images, and code, responds to natural language questions, so any employee can use it.
Is very good at understanding different types of data - useful given councils have large amounts of unstructured data in a large variety of formats.

11.7 Use

This policy applies to all staff using any GenAI tools, whether through council-owned devices or personal devices used for council activities. These tools can be embedded in other tools – such as email clients or video conferencing tools. For example, Microsoft 365 includes many authorised GenAI tools – such as Teams transcription.
Use of GenAI must be in a manner that promotes fairness and avoids bias to prevent discrimination and promote equal treatment and be in such a way as to contribute positively to the council's goals and values.
Staff may use GenAI for work-related purposes if they adhere to this policy. This includes tasks such as generating text or content for reports, emails, presentations, images and customer service communications.
Particular attention should be given to Governance, Vendor practices, Copyright, Accuracy, Confidentiality, Disclosure and Integration with other tools.

11.8 Governance

Before entering any kind of personal or confidential information into a GenAI website, tool or app, staff must first complete a Data Protection Impact Assessment detailing their intention to use, the reason for use, and

the expected information to be input as well as the generated output and distribution of content.

11.9 Vendors

Any use of GenAI technology in pursuit of council activities should be done with full knowledge of the policies, practices, terms and conditions of the developers or vendors of that tool.

11.10 Copyright

Staff must adhere to copyright laws when utilising GenAI. It is prohibited to use GenAI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material. If a staff member is unsure whether a particular use of GenAI constitutes copyright infringement, they should contact Legal Services or Information Governance Team before using GenAI. For example, using GenAI to produce a logo could produce something based on a copy of a logo that is a trademark or is copyrighted.

11.11 Accuracy

GenAI can completely make up "facts". They will have ingested a large amount of data sources, some of which may be fiction. They also generate text that looks like real facts. So, it is important to fact check any content produced.

All information generated by GenAI must be reviewed and edited for accuracy prior to use. Users of GenAI are responsible for reviewing output and are accountable for ensuring the accuracy of GenAI generated output before use/release. If staff have any doubt about the accuracy of information generated by GenAI, they should not use GenAI without correction.

11.12 Confidentiality

Confidential and personal information must not be entered into a public GenAI tool (such as ChatGPT, Bing etc.). This is because the information will then enter the public domain and may be used for further training of the publicly available tool. This would amount to a data breach. Staff must follow all applicable data privacy laws and organisational policies when using GenAI. For example:

- Staff must not use an unauthorised GenAI tool to write a letter to a customer with any personal details in. For example: 'Mr J Bloggs at 123 High Street' as that data will be ingested and kept by the GenAI for re-use.

- Staff must not use GenAI apps on personal phones to record and summarise work meetings, or to use translation services.
- Staff must not upload spreadsheets full of customer data for GenAI analysis.

If staff have any doubt about the confidentiality of information or what will happen to the data they enter, they should not use that GenAI tool. Confidential or personal data should only be entered into a GenAI tool that has been approved and procured specifically for 'The Parties' use where the data entered is confined for 'The Parties' sole use and use of that tool has been specifically sanctioned for that purpose by the Data Protection Officer and ICT. So, for example, using Microsoft Teams with a council login to transcribe meetings is authorised. However, using a free tool downloaded to a personal phone to transcribe a work meeting is not authorised and could constitute a data breach.

11.13 Social Impact and Equality

Staff must be aware of how the use of GenAI may impact different groups of people in different ways as it may have inherent social bias or have been trained on stereotypes. It may have inappropriate cultural values or display sensitive content. For example, GenAI must not be allowed to solely determine which customers should have access to services; Humans must be involved in such decision-making where needed, and there must be an appeal processes for any automated or AI-informed decisions. This process will be undertaken by the Information Governance & Risk Team.

11.14 Ethical Use

GenAI must be used ethically and in compliance with all applicable legislation, regulations, and organisational policies. Staff must not use GenAI to generate content that is discriminatory, offensive, or inappropriate. If there are any doubts about the appropriateness of using GenAI in a particular situation, staff should consult with their supervisor or Information Governance Team.

11.15 Disclosure

Content produced via GenAI must be identified and disclosed as containing GenAI-generated information.

Footnote example:

Note: This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the author for accuracy

and edited/revised where necessary. The author takes responsibility for this content.

11.16 Integration with other tools

API and plugin tools which enable access to GenAI and extended functionality for other services (such as email, Teams or search engines) must not be used unless approved by the Data Protection Manager and ICT.

API and plugin tools must be rigorously tested for:

- Moderation – to ensure the model properly handles hate, discriminatory, threatening, etc. inputs appropriately.
- Factual responses – provide a ground of truth for the API and review responses accordingly.

11.17 Risks

Use of GenAI carries inherent risks. A comprehensive risk assessment should be conducted for any project or process where use of GenAI is proposed via a data protection impact assessment and an ICT Security assessment. The risk assessments should consider potential impacts including legal compliance; bias and discrimination; security (including technical protections and security certifications); and data sovereignty and protection.

GenAI may store sensitive data and information, which could be at risk of being breached or hacked. The council must assess technical protections and security certification of a GenAI tool before use. If staff have any doubt about the security of information input into GenAI, they should not use GenAI.

11.18 Legal compliance

Data entered into GenAI may enter the public domain. This can release non-public information and breach regulatory requirements, customer, or vendor contracts, or compromise intellectual property. Any release of private/personal information without the authorisation of the information's owner could result in a breach of relevant data protection laws. Use of GenAI to compile content may also infringe on regulations for the protection of intellectual property rights. Staff should ensure that their use of any GenAI complies with all applicable laws and regulations and with council policies.

11.19 Data sovereignty and protection

While a GenAI platform may be hosted internationally, under data sovereignty rules information created or collected in the originating country will remain under jurisdiction of that country's laws. The reverse also

applies. If information is sourced from GenAI hosted overseas, the laws of the source country regarding its use and access may apply. GenAI service providers should be assessed for data sovereignty practice by any organisation wishing to use their GenAI.

11.20 Compliance

Any violations of this policy should be reported to the council's Information Governance Team or senior management. Failure to comply with this policy may result in disciplinary action, in accordance with council's Human Resources policies and procedures.

11.21 Review

This policy will be reviewed periodically and updated as necessary to ensure continued compliance with all applicable legislation, regulations, and organisational policies.