APPENDIX 11

The Golden Rules

May 2018

Information Security– Golden Rules

Information is a valuable asset. The Council has a duty and responsibility to protect it. This responsibility is placed on the Council by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) and monitored and regulated by the Information Commissioner's Office.

The Information Commissioner has powers to impose monetary penalty notices for up to €20,000,000 for breaches of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR), along with having the authority to carry out assessments of organisations to ensure their processes follow good practice. The key guidance document that the Council would be measured against is the Local Public Services Data Handling Guidelines 2017 by the Public Services Network.The Council wants to comply with these guidelines to ensure good practice is being followed. The Council needs to ensure that everyone uses and manages information assets and information systems in an effective, efficient, and ethical manner.

The objective is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities. The Council is committed to protecting information through preserving:

Confidentiality - Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities or processes.

Integrity - Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability - Being accessible and useable on demand by an authorised individual, entity or process.

It is essential that you understand your data protection and security obligations and that every day business practice helps foster an organisation wide security-aware culture embracing good data/information handling behaviours.

These Golden Rules aim to help you:

- safeguard the Council's valuable information assets, systems and equipment;
- use information assets responsibly within the framework of the law;
- make sure you understand the corporate policies with which you must comply; and
- signpost the mandatory corporate on-line training you must undertake.

All employees must comply with the minimum corporate security standards set out in these rules which are based on the Council's Information Governance Framework of policies, procedures, standards and guidance and also ensure you follow any localised business specific data handling requirements.

Protected Information is any information which is:-

- personal/sensitive personal information; or
- confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

Personal information: is any personal data as defined by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of

personal information held by it as governed by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR).

Sensitive personal information:is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- mental/physical health or condition
- sexual life
- a committed or alleged offence
- details of the proceedings or the sentence of any court

You are personally accountable for safeguarding and using the Council's information assets responsibly and appropriately. Make sure you understand the rules for handling the information, systems and equipment in your care and stick to those rules rigidly.
Rule 1 – Respecting "need to know" principles
Rule 2 – Avoiding inappropriate disclosure
Rule 3 – Keeping your passwords safe
Rule 4 – Storing data securely
Rule 5 – Working securely in the office
Rule 6 – Working securely on the move and away from the office
Rule 7 – Working safely on line
Rule 8 – Sending protected information securely
Rule 9 – Disposing of protected information securely
Rule 10 – Undertaking mandatory on line training
Rule 11 – Reporting incidents
Rule 12 – Preventing security incidents

Rule 1: Respecting "need to know" principles

- Only access protected information if it is part of your job and you have a legitimate business need to know.
- Never access protected information for personal interest or gain.

- If you need protected information 'owned' by another business area to do your job, make sure you are authorised to ask for it, you only ask for the minimum necessary for the required purpose and, you are clear why you are entitled to it.

Rule 2: Avoid inappropriate disclosure

- Before disclosing protected information to an external third party always ask yourself *"is this request legitimate?"* and verify that the requester is who they say they are.
- Always make certain you have the legal authority, including the legal power to disclose the information.
- Check whether the purpose could be satisfied with anonymised rather than protected information.
- Keep a documented audit trail of all ad hoc disclosures.
- If you are unsure of the rules, check with your manager, Legal Services or Risk Management and Audit Services.
- Check whether you need consent to share or if sharing is governed by a legal gateway.

Rule 3: Keeping your passwords safe

- Protect passwords at all times.
- This applies to all passwords enabling access to data and to the Council's network, business systems, email and the internet.
- Avoid writing your password down and if you have to, don't leave it in obvious places such as under your keyboard, next to your monitor or other easily searchable places.
- Ensure that your password is sufficiently complex that you can remember it but it cannot easily be guessed by others.
- Immediately change your password if you suspect it may have been compromised.
- Please refer to the ICT Freshdesk.

Rule 4: Entering and storing data securely

- Enter data accurately and completely.
- Physical files containing protected information must be locked away securely.
- Always save electronic files on the Council's network drives and do not keep the information on your local computer hard drive.
- Remember the secure network is automatically backed up and remains available even if your computer fails.
- If you are working away from the office, access to view or amend data should be via a secure remote connection to Tameside's network.
- If this is not possible and permission is granted to create or store protected information on encrypted portable devices or removable media, this must be the minimum necessary for the approved business purpose.
- The authorised user is responsible for ensuring that unique data held on encrypted devices is regularly backed up to the Council's secure network.
- Information assets must be managed in accordance with the retention and disposal guidelines. Once no longer required for legal, regulatory or business purposes, information should be securely disposed of in line with the retention and disposal schedules for your service area.
- Only retain the minimum necessary information for the minimum period of time.

Rule 5: Work securely in the office

- Never leave protected information or other valuable assets out on your desk when you are not around.
- Remove documents from printers and copiers as they are produced to avoid them being picked up by mistake, or read by someone else.

- When sending information by post check that you have only included the correct documents, especially if collected from shared printers/copiers.
- Lock your work station, log off at the end of the day and switch off your screen.
- Lock windows, offices and conference rooms containing physical records and computer equipment whenever the area is unoccupied.
- Wear your pass when you are in Tameside buildings, remove it and keep it safe when you leave.
- Challenge anybody you see in your building who is not wearing an appropriate security pass.

Rule 6: Work securely on the move and away from the office

- If you are authorised to carry protected information in paper files and/or on encrypted devices beyond your secure workplace keep your laptop, mobile device, and official papers with you at all times and take reasonable precautions based on the environment you are in.
- Ensure that you:
  - comply with local physical file tracking procedures;
  - make sure your laptop is protected with encryption software;
  - avoid *"shoulder surfers"* in public places viewing your screen or confidential business conversations being overheard;
  - do not leave protected information or equipment in an unattended vehicle (unless securely locked in the boot); and
  - limit the risk of valuable information or equipment being lost or stolen (i.e. by not taking council resources to places where they are at risk of being stolen).
- Always ask yourself the question *"Do I really need to take protected information out of the office?"* The best way to prevent theft or accidental data loss is to leave it safely on Council premises.
- Only take the minimum necessary paper records with you (rather than the whole file).
- Do not let unauthorised people, including family members, use or view valuable council resources.
- If you have encrypted equipment and protected information in physical files overnight in your home, reduce the risk by ensuring that the unencrypted physical files are locked away separately.

Rule 7: Working safely on line

- Make sure you understand the Council's internet and email policies.
- Never open an email from sources you do not know and trust.
- Always report any unusual email messages or suspicious attachments or links especially in unsolicited emails.
- Never use non-Tameside email accounts to send or receive protected information.
- Follow the ICT Security Policy.

Rule 8: Sending protected information securely

- Be diligent when sending letters, addressing envelopes, choosing fax numbers and email addresses to prevent errors and misdirection.
- Try to limit the harm which might be caused if something goes wrong by thinking about whether you need to reiterate sensitive details (i.e. identifiers or bank account numbers the recipient has previously supplied) and send only what you absolutely need to send and no more.
- Do not send protected information by external email ***UNLESS***:
  - You have a GCSX account and are sending it securely to another GCSX mail account (or any of the other secure government networks);***or*** You are sending it in an attachment, using strong password protection and encryption software such as Egress Switch.

- If you are sending protected information by internal email, within the Council's secure network, always check you have addressed the email correctly to avoid sending it to the wrong person.
- Do not send protected information to a generic mail address unless appropriate and you actually know the mail address relates only to a Tameside internal mail account.
- Only transport protected information on removable media (cameras, DVDs, memory sticks etc.) if you are using Council supplied devices and obtain assurance that the device or the information stored on it, is encrypted to recognised industry standards.

Rule 9: Disposing of protected information securely

All resources containing protected information must be disposed of securely. This applies to protected information held in various formats including:

- paper records (e.g. printed notes, assessments, correspondence or reports).
- electronically stored on encrypted laptops and other portable devices.
- stored on approved removable media, for example writable CDs, writable DVDs, external hard drives, audio and video tapes.

Portable laptops that are no longer required must be returned to ICT enabling the hard drive to be permanently erased with specialist software before disposal or recycling to another business area.

Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Service for secure disposal.

Confidential paper waste must be kept separate from ordinary paper waste and protected from accidental loss, damage or unauthorised access until its final removal/disposal. Follow the minimum standards in the Council's corporate policy for disposing of waste, as supplemented by locally agreed business operating procedures.

Particular care must be exercised during office relocations and moves to ensure that all confidential paper waste and non-required ICT equipment is disposed of properly.

Rule 10: Training

On line Data Protection and Information Governance training is available via the MeLearning portal and is mandatory for all staff.

A Data Protection video produced by the ICO is available on the Information Governance pages on the Staff Portal as an additional resource.

Specific workshops are available on request. Please contact the Risk Management and Insurance team to discuss.

Further guidance and resources are available on the Staff Portal under Information Governance.

Rule 11: Reporting Incidents

You must always report actual or suspected security violations, problems or vulnerabilities to the ICT Security Officer (Ext. 2773) as soon as possible.

If the incident or near miss, involves the loss, theft or unauthorised disclosure of protected information it must be reported immediately via the Incident Reporting Procedure.

Delaying reporting an incident makes it more difficult to solve the problem. Report it straight away so your manager, ICT, Legal Services and Risk Management and Audit are able to act quickly and get any expert advice they may need.

If an incident is reportable to the ICO it needs to be completed within 72 hours.

Rule 12 – Preventing security incidents

Remember good data security is in your interest too.

Security breaches caused by deliberate, negligent or reckless behaviour could result in disciplinary action, dismissal and even give rise to personal fines (up to £50,000) and criminal offences. Make sure you observe the Council's confidentiality, data protection and information governance rules. This will help avoid misuse, unauthorised disclosure, modification, loss or theft of protected information assets which can harm individuals, commercial/partner organisations and/or the reputation of the Council.

Work Securely

These Golden Rules apply whether you are in the office, working remotely or on the move. They aim to ensure you play your part in ensuring our information and information systems are not compromised. Be security alert at all times and do not exceed your access privileges or authority.