APPENDIX 2

HILLINGDON
LONDON

Protecting personal information

Golden rules for protecting personal and sensitive data

May 2018

The Council has a duty to protect the information held about members of the public. Breaches of the Data Protection Act 2018 (DPA) and the General Data Protection Regulations (GDPR) can result in enforcement action being taken against the Council by the Information Commissioner's Office and a fine of up to 20 million Euros being imposed. This is turn can lead to disciplinary action being taken against individual members of staff responsible for the data breach.

Always follow the Golden Rules for protecting personal and sensitive data:

1. **Always keep personal information safe and secure**
2. **Check who you are sharing information with**
3. **Use email carefully and responsibly**
4. **Do not store personal data on laptops and mobile devices**
5. **Keep data secure when working away from the office**
6. **Take extra care when taking information out of the office**
7. **Always report information security breaches**

1. Always keep personal information safe and secure

- Always ensure that records containing personal and sensitive data are stored securely to prevent unauthorised access. If you have paper records you must store these in a locked cabinet or drawer. You can see the definition of *personal and sensitive data* in the Council’s Data Protection Policy.

- Do not use the hard drive (the C: drive) on your desktop computer or laptop for saving and storing personal data as this is not secure and back-up copies of records are not made by ICT networks.

- Never share any of your ICT systems passwords with anyone else. Passwords should not be written down. Passwords should be a minimum 8 characters in length and use a mix of letters, numbers and other characters. Do not use the same password for different programmes.

- Ensure that your desk and computer cannot be overlooked by members of the public. Where you are processing sensitive personal information you should also consider whether care should be taken to prevent other members of staff from seeing the work.

- Be *security aware* when entering or leaving the office. Do not let unauthorised persons into the building. If someone asks to be let into the office or tries to follow you through the secure doors politely ask to see their ID or show them to the Security Desk where the security team will be able to assist them.

- When records no longer need to be kept (in line with the Council’s Document Retention and Destruction Policy), all personal information held in hard copy should be disposed of appropriately using the confidential waste bins provided or by using a shredder where available.

- When using the printer, photocopier or scanner please check that all documents are collected when you have finished. Check that the documents you pick up are the correct ones.

- Before sending a letter <u>always</u> check that the address is correct and that it is addressed to the correct recipient. Double-check any documents that are being enclosed to make sure they are the correct ones.

- You should avoid sending sensitive records by fax unless there is no other secure alternative. Before sending a fax check with the recipient that the fax number is correct and make the recipient aware that the fax is being sent. Always take care to ensure that the correct number is inputted into the fax machine. You may wish to ask a colleague to assist you.

- You must only use authorised Council USB memory sticks. The use of any other device with Council equipment risks damaging systems. Contact your Business Support team or the ICT Service Desk for assistance with this.

2. Check who you are sharing information with

- If you are sharing personal and/or sensitive data, you must make sure that the person you are sharing the data with has a need and right to have access to the data. The disclosure of data must be authorised by the owner of that information (asset) and lawful.

- Be careful about sharing information via telephone. Take simple steps to verify the caller's identity to establish their identity.

- Requests for disclosure by law enforcement agencies should be made in writing.

- Members of staff must only access personal information and systems where it is necessary for their role. Remember - it is a disciplinary offence to use or access the Council's records for your own purposes.

- Do not discuss or share Council-owned personal data via social media. Only authorised members of staff should use social media for Council purposes.

3. Use email carefully and responsibly

○ All email for Council business must be sent using the Council's email systems. Messages containing very personal or large amounts of sensitive data must be sent using "Egress". Personal email accounts must not be used for council business.

○ When sending an email, care must always be taken to ensure that it has been addressed to the appropriate person and that the correct email address has been used.

○ When sending bulk email it is important to use the blind carbon copy function (Bcc) to prevent the inadvertent disclosure of email addresses.

○ When sending emails involving sensitive content, use simple anonymisation techniques to mitigate the risks of unauthorised or accidental disclosure. For instance, use reference numbers and initials rather than names. The intended recipient will know who the information relates to but an unintended recipient will not be able to identify the subject of the email.

○ Be aware of the risks posed by spam email containing viruses and malware. Whilst the Council has good anti-virus software in place, members of staff should be alert to any email that seems odd or unusual, for instance it looks out of place, poorly spelt, contains an offer that is too good to be true etc. If you receive a suspect email do not click on any link or open an attachment it may contain but report it to ICT immediately.

4. Do not store personal data on laptops or mobile devices

○ Personal data should only be stored on the Council's secure network.

○ Due care and attention should be used when working on laptops or other devices when away from your normal place of work. Make sure you cannot be overlooked and never leave your equipment unattended or lend it to a 3rd party.

○ Only use Council issued or Council approved laptops or mobile devices. If you are using your own mobile device then this must have been approved in accordance with the Council's Bring Your Own Device Policy (BYOD).

5. Keep data secure when working away from the office

○ Files, paperwork and mobile computing devices must be stored in a secure location when not in use. Store any manual records separately from your ICT equipment.

- Council data should not be stored at home long term. If you are to be out of the office for a significant period of time, you should ensure that all Council owned personal data are returned to the office.

- If you are leaving the Council's employment you must return all Council owned data and equipment to the Council in good time.

- A record of any files or records taken out of the office should be kept in case they are damaged/destroyed, lost or stolen. Where possible you should avoid taking original files or records out of the office.

6. Take extra care when taking information out of the office

- The Council recognises that there are circumstances when personal information will need to be taken out of the office.

- Only transport the minimum of personal information required. Ensure that you don't leave files, equipment or bags containing Council equipment or Council personal data unattended at any time or on view in a locked vehicle.

- When travelling with personal data, ensure that files are always carried in a sturdy locked bag.

- When travelling on public transport, extra care should be taken to ensure that bags containing personal information are not lost or stolen.

- You must ensure that any electronic media has been appropriately encrypted. Only Council owned electronic transportable media should be used.

- Data being delivered by electronic media should be either hand delivered and a receipt obtained, or sent by courier/recorded post.

- The password (encryption key), which provides access to information being sent by any electronic media or email, must be sent to the recipient by a different method to that by which the data has been sent.

- It is good practice to keep a record of any large-scale data transfers. The record should show what data was sent, how it was sent, and what security measures were taken. All large-scale transfers of personal data must be authorised by Heads of Service of the information asset owner. If in doubt, seek legal advice from the Council's Statutory Data Protection Officer.

- Where possible you should avoid working on or discussing work involving personal or sensitive matters in a public environment. If this is not possible, care should always be taken to ensure that you are not overlooked or overheard.

7. Always report information security breaches

- **All staff have a responsibility to report a suspected or actual breach of confidentiality or loss of data**. Early notification of an incident can ensure that any mitigating or recovery actions can take place as soon as possible. It is better to report a suspected incident even if you are unsure if one has occurred, than not to do so.

- **If you suspect an information security breach has occurred, you should report it immediately to your line manager and your service manager.**

- Service managers must report the incident to the Council's Statutory Data Protection Officer and notify their Head of Service immediately.

- Breaches will be dealt with in line with the Council's Procedure for Reporting Information Security Breaches, Data Protection Breaches and Card Security Incidents.

- **There is a statutory duty on the Council to notify the Information Commissioner's Office of the above within 72 hours. Failure to do so can result in a fine of up to 10 million Euros being imposed on the Council.**