Information, Technology and Systems – Acceptable Use Policy (AUP)

The acceptable use policy is mandatory for all users of Harrow Council (hereafter referred to as 'the Council') information or information technology (IT) systems, including members, employees, temporary workers, **volunteers,** contractors and any authorised 3rd parties (hereafter referred to as 'individuals').

The policy sets out the acceptable standards in using and implementing IT systems and other Information Assets. You are required to read, understand and accept this policy before being granted access to the IT systems.

The council proactively monitors the use of its IT systems. Any actual or suspected breaches of this Policy within, or affecting the council's systems or information (electronic or manual based) will be dealt with under the council's disciplinary procedure.

If you are not directly employed by the council, i.e. a volunteer you must adhere to the rules in this policy. If you do not comply with the rules in the policy, then your access to the Council's information resources will be removed. If there is evidence that you have committed a criminal offence through your use of the Council's systems or equipment, you could be prosecuted.

We all have a responsibility to protect the Council's information, devices and equipment at all times to prevent theft or loss. You must take reasonable precautions to ensure the Council's information paperwork and laptop, phone or any other devices are protected at all times.

Security breaches caused knowingly, by reckless behaviour, or non-compliance with this policy or any other information governance and security policies including the non-reporting of an incident, may result in disciplinary action.

You should also familiarise yourself with the Information Governance and Security Policy available on the hub.

The terms 'data' and 'information' are synonymous.

Access to Systems and Information Management

1. Only access information you are authorised to do and relevant to your work.

2. Accessing or attempting to gain access, copying or removing information (including photos) without a business reason and prior authorisation from senior management is forbidden and shall be deemed a disciplinary offence.

3. When access to information is authorised, you must ensure the confidentiality and integrity of the information is maintained.

4. Ensure the information and systems are adequately protected in accordance with Council policies, legal and statutory requirements (including compliance with the requirements of General Data Protection Regulation (GDPR) and other data protection laws).

5. Information must be stored in the relevant line of business system and this information shall not be duplicated in other storage areas.

6. Team specific information shall not be stored in personal drives, such as H drive or MyFiles site.

7. Personal files such as music, videos, and photographs must not be stored on the Council's storage area.

8. The Council does not allow access to and/or storage of any information on non-approved 3rd party sites or internet online storage/cloud services i.e dropbox, googledocs. Exceptions to organisation policy will be assessed and handled on a case by case basis after a risk review and if approved, will only be granted for a limited period (or the alternative of having the data downloaded by IT)

9. Harrow Council encrypted devices must be used when processing and carrying out Council duties.

10. Personal and sensitive information must not be stored or processed on a personal or privately owned device or non-council email systems.

11. Username and passwords must be kept secure and must not be shared with anyone (this includes managers and IT staff).

12. Never allow anyone else to use your username and password

13. Never use another colleague's username and password to access Council systems and information.

14. All Council devices (e.g. workstations/laptop/mobile) must be 'locked' (using the Ctrl-Alt-Delete function or other applicable method) when left unattended.

15. Observe a clear desk policy when dealing with personal and sensitive information and ensure that it is not left unattended on desks.

16. Dispose of all paper documents in the secure waste bins provided.

17. Take care when sharing information with external partners or the public. Send the information to the named recipient and to the correct address.

18. Only material that is publically available should be published on the Harrow website. Ensure information that forms part of a document, which contains personal and sensitive information, is redacted prior to publication.

19. If information has been redacted, ensure that it cannot be reversed. Further information on Redaction can be found on the hub.

20. Mobile or removal devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Council authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Internet, Email, Instant Messaging and Social Media

21. The Council email system must be used to conduct Council business. Individuals are accountable and personally responsible for their actions on the internet and emails sent from their account.

22. All user/email accounts are deleted when they have been inactive for 3 months - this follows best practice in terms of security and integrity of the system.

23. The Council's email system must only be used as a means of communication and transmission. Emails containing information and attachments that need to be retained for evidential purposes must be saved in the relevant system and deleted from the email system.

24. A secure email transmission method must be used when sending personal and sensitive information and attachments to external recipients.

25. Emails and attachments that contain personal or sensitive information must never be sent to a personal email account (for example, to work remotely on a personal device).

26. Emails to Members must be sent to their 'harrow.gov.uk' email account and not to their personal email account. Certain nominated officers may send non-personal or sensitive information on logistical matter (e.g. arranging meetings) to a Members personal email account. Full details of nominated officers can be found on the hub.

27. The data allowance and/or internet bandwidth provided (via a dongle or any other mobile device) must only be used for Council business and must be used responsibly.
28. Email, instant messaging, internet and other social media (such as Facebook and Twitter) must be used responsibly. Always use professional and appropriate language in all messages and conversations.

29. Do not use any language or post messages (including images) that are abusive, threatening, harassing, discriminatory or otherwise offensive. This includes forwarding any received email. If you receive any messages of this nature from another employee or other outside organisations, inform your line manager immediately.

30. The use of internet, council email, telephones, Council WiFi and any data allowance (such as a dongle), landlines and mobile devices you may have are intended for business use. Only limited personal use is acceptable, outside of working hours, that does not affect the individual's business performance, is not detrimental to the Council in any way e.g. create additional cost, not in breach of any terms and conditions of employment and does not place the individual or the Council in breach of statutory or other legal obligations.

31. Access to personal email accounts is not permitted on the council's network.

Working Off-Site

32. Papers and devices taken off-site should be protected in transit, not left unattended in public places and must be stored securely. Consider using a secure lockable bag.

33. Papers and devices left in unattended vehicles must be out of sight, locked away securely in the boot and never left overnight.

34. Papers taken off-site must be returned to the Civic for secure disposal or cross shredded and must not be disposed of in domestic bins.

35. Council devices must be used when working remotely. Unknown or untrusted public WiFi hotspots must not be used.

36. Take precautionary measures to prevent unauthorised disclosure of information through "shoulder surfing" i.e. someone looking over your shoulder to view information that they have no right to read.

37. Do not leave you council computer, laptop or any other device unattended in such a state as to risk unauthorised viewing of information displayed on it.

Physical Security

38. Council identity (ID) passes must be worn at all times, shall be visible and not shared with anyone else. Visitors must be signed in and must be escorted at all times.

39. Members of staff are required to have their photographs taken upon commencement of employment for security and identification purposes. Therefore they are deemed by the Council to have provided consent for their photographs to be uploaded and displayed on the internal IT system for applications such as emails, Outlook, Lync and any other internal business related resources,

Working with Third Parties and Information Sharing

40. An Information Processing, Information Sharing or Non-Disclosure agreement must be in place before any personal or sensitive information is shared with a third party. A Code of Connection (Coco) agreement is required between the council and any 3rd Party before any access is permitted to the Harrow Council network. Further information on sharing information can be found on the hub.

Reporting Security Incidents and Breaches

41. Security incidents and breaches must be reported immediately to the line manager and the ICT Service Desk on ext. 2000 or 020 8424 1000. Further information on Security Incident and Breaches Reporting can be found on the hub.

42. If you are a line manager you must ensure that you follow the incident reporting procedure and that any incident / breaches reported to you are investigated and resolved.

Training

43. The Information Governance and Security Awareness e-learning training must be completed within 1 month of the individuals start date and thereafter, annually.

Actions upon Termination of Contract

44. All Council equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, RSA tokens etc., must be returned at termination of contract.

45. Line mangers must make every effort to ensure that all Council equipment has been returned.

46. All Council data or intellectual property developed or gained during the period of employment remains the property of the Council must not be retained beyond termination or reused for any other purpose.

Monitoring and Exception of Privacy

47. The council's network and systems are often monitored and logging will take place where appropriate and is maintained for legal regulatory and policy compliance as well as system maintenance purposes.

48. Investigations will be carried out where reasonable suspicion exists of a breach of this or any other policy. Harrow Council has the right (under certain conditions) to monitor activity on its systems, including internet, email and phone use, in order to ensure systems security and effective operation, and to protect against misuse.

49. Any monitoring will be carried out in accordance with audited, controlled internal processes, legislation and other regulatory requirements.

50. Whilst the council desires to provide a reasonable level of privacy, individuals should be aware that the information they create and process on the corporate network and systems remains the property of Harrow Council. Due the need to protect the council's network and information, management cannot guarantee the personal privacy of information stored on any council system.

Agreement

I confirm that I have read, understood and accept this policy.

Print Full Name:

Date:

Signature: