## SOFTWARE ACCEPTABLE USAGE POLICY

<table>
<thead>
<tr>
<th>Author:</th>
<th>Tee Patel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner:</td>
<td>IGB</td>
</tr>
<tr>
<td>Version:</td>
<td>1.3</td>
</tr>
<tr>
<td>Classification:</td>
<td>OFFICIAL</td>
</tr>
<tr>
<td>Issue Status:</td>
<td>Approval</td>
</tr>
<tr>
<td>Date of First Issue:</td>
<td>21/01/2008</td>
</tr>
<tr>
<td>Date of Latest Re-issue:</td>
<td>30/04/2020</td>
</tr>
<tr>
<td>Review Date:</td>
<td>18/11/2019</td>
</tr>
<tr>
<td>Reviewer:</td>
<td>Steve Durbin</td>
</tr>
<tr>
<td>Date of Next Review</td>
<td>30/04/2021</td>
</tr>
<tr>
<td>Date of IGB Acceptance</td>
<td>30/04/2020</td>
</tr>
</tbody>
</table>
This page has been left intentionally blank
Distribution List: This document is for distribution to all individuals and companies as mentioned within the Scope of this Policy. This document is subject to FOI.

Document History

<table>
<thead>
<tr>
<th>DATE</th>
<th>ISSUE NUMBER</th>
<th>REVISION DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 Jan 2008</td>
<td>1.0</td>
<td>New</td>
</tr>
<tr>
<td>27 Sep 2017</td>
<td>1.1</td>
<td>Revisions for GDPR and changes since 2008</td>
</tr>
<tr>
<td>31/07/2018</td>
<td>1.2</td>
<td>Annual review</td>
</tr>
<tr>
<td>26/03/2019</td>
<td>1.3</td>
<td>IGB approval</td>
</tr>
<tr>
<td>18/11/2019</td>
<td>1.4</td>
<td>Annual review</td>
</tr>
<tr>
<td>30/04/2020</td>
<td>1.5</td>
<td>IGB Approval</td>
</tr>
</tbody>
</table>
CONTENTS

1.0 Introduction ........................................................................................................... 5
  1.1 What is Information? .................................................................................... 5
  1.2 What is the Security Approach? ................................................................. 5
2.0 Scope ...................................................................................................................... 5
3.0 Software Acceptable Usage Policy (SAUP) ...................................................... 5
4.0 Enforcement Monitoring .................................................................................... 6
  4.1 Penalties for Non-compliance .................................................................... 6
  4.2 Enforcement ................................................................................................. 7
  4.3 Exceptions to the Software Acceptable Usage Policy .............................. 7
  4.4 Non-compliance .......................................................................................... 8
1.0 Introduction
Information is a valuable asset and is an essential requirement for a local authority to carry out its legal and statutory functions. The information Enfield Council processes is about you, it can be highly confidential and very personal; therefore the Council has a legal duty to take care of it. This document will address why the Council needs to secure the information we process, identify the security measures required and provide guidance to users of Council information.

1.1 What is Information?
Information can be in a number of forms: -

- Spoken in conversations (including telephone)
- Printed out and or written on paper
- Sent by fax
- Sent via E-mail
- Sent via texts (SMS), instant messages (IM)
- Stored on computers
- Transmitted across networks
- Stored on media (tapes, disks, CD’s, film, microfiche etc.)
- Stored in databases
- As part of presentations
- Any other methods used to convey information and knowledge.

1.2 What is the Security Approach?
The most effective way of providing information security is to use a structured approach that will ensure the appropriate controls are applied to specific areas rather than general controls to all areas. The key standards in the area are the ISO27000 series. These standards provide a comprehensive set of security controls comprising the best information security practices in current use. The objective os to provide organisations with a common basis for providing information security and to enable information to be shared between organisations.

2.0 Scope
This Software Acceptable Usage Policy (SAUP) applies to all Enfield Council’s systems and is effective from the date of issue of this document. The policy, rules and conditions apply to all Enfield Council Members, employees, contractors, consultants, agency staff, independent contractors and other users of Enfield Council information systems irrespective of the platforms used or where they are located.

3.0 Software Acceptable Usage Policy (SAUP)
Enfield Council is committed to the use of authorised software within its computer systems. It is expressly forbidden for ‘users’ to load or operate software gained from the Internet, magazines or other sources. The Council is also committed to using software for which it has current licences.
Where software is developed and/or modified in-house, under licence agreement, it should only contain the functionality that was specified in the requirement and must not contain functions that have fraudulent or mischievous intent (generally referred to as Malware).

It is the responsibility of all users to ensure that they do not introduce viruses into computer systems. Users should take care when receiving electronic information from unknown sources, including attachments within E-mail. Where there are reasons to access information from questionable source(s), active virus checking must be performed, preferably on a standalone computer and/or test server, thus having no communication links to other systems.

The following provisions, which apply to the use of all computers, govern all users: -

- Only software purchased by Enfield Council and through IT may reside on Enfield Council computer equipment.
- IT will undertake to purchase licences for all products used by Enfield Council and will control the allocation of licences for products that are distributed as single media items and licences for multiple instances of that one distribution.
- Only software approved by IT may reside on Enfield Council computer equipment and / or telecoms equipment including smart phones and smart devices.
- Only IT authorised technical staff may install or remove software on Enfield Council computer equipment.
- Software includes source code, object code and intermediate code that can be firmware as well as software.
- Downloading of “shareware” and/or “freeware” is prohibited irrespective of the fact that a licence may or may not be needed unless IT has approved the product to be downloaded and installed.
- The installation of personal software including screen savers is prohibited.
- Upgrades to software products will be treated as new products.
- All software media is to be held and securely stored by IT.
- IT may copy software media only if they are legally allowed to do so and where approved by the IT Security Analyst. This is in accordance with Copyright laws and the terms and conditions of the relevant software license. Software media may not be copied under any other circumstances.

4.0 Enforcement Monitoring

Monitoring of the standard is the responsibility of all managers as part of their management role. The Internal and External Audit may undertake reviews on a planned and ad-hoc basis as part of the audit process. The IT Security team will conduct quality reviews on cyclical basis as part of their security role.

4.1 Penalties for Non-compliance

The Council has an established staff Disciplinary Code of Conduct. Any breach of policies contained within this document will be dealt with in accordance with those procedures.
4.2 Enforcement
A violation of standards, procedures, or guidelines established in support of this policy will be brought to the attention of the IT Security Analyst for investigation. The IT Security Team enforces this policy by continuously monitoring, through the use of software tools. Business Unit Management, Human Resources, Internal Audit and External Audit will be notified when it is considered a breach has taken place. It is the responsibility of all users (as defined within the Scope of this document) to ensure compliance with the policy. Failure to adhere to the policy may result in a breach of Financial Regulations, Standing Orders and or current legislation. In the event of a breach by a Council employee, IT facilities may be suspended/removed and disciplinary action taken against them in accordance with the Disciplinary Code of Conduct. A breach of the Software AUP may be considered as a gross misconduct offence and lead to a penalty up to and including dismissal. Action against non-Enfield employees may result in removal/suspension of IT facilities, removal from site, cancellation of any contracts and possible legal action.

4.3 Exceptions to the Software Acceptable Usage Policy
The Council expects all users to achieve compliance with the directives presented within this policy. In the following exceptional cases, compliance with the Council’s Information Security policies may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question. These exceptional circumstances are outlined below:

- If complying with the policy would lead to physical harm and/or injury to a member of staff or other third party (e.g. contractor).
- If complying with the policy would cause significant damage to the Council’s reputation and/or ability to operate
- If an emergency arises and a user has no alternative other than to breach Council policy to assist with the emergency.

In such cases, the Council employee or third party (contractor etc) concerned must take the following action:

- Ensure that a Business Unit Manager is made aware of the situation and the action to be taken.
- Ensure the situation and the actions taken are recorded in as much detail as possible
- Ensure the situation is reported to the IT Security Analyst as soon as possible.
  *(Failure to take these steps may result in disciplinary action).*

The IT Security Analyst will:

Maintain a list of known exceptions and non-conformities to the Information Security Policies. This list will contain:

- 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 Information Security Policies are not considered applicable.
• The Council will not take disciplinary action in relation to known, authorised exceptions to the Information Security Policies.

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

• A breach of the Council’s Information Security Policies, standards or controls. Unauthorised disclosure or viewing of confidential information belonging to the Council
• Unauthorised modification to information, software or operating systems
• The use of hardware, software, communication networks, equipment, data or information for illicit purposes, which may include violations of law, regulation or reporting requirement of any enforcement agency or government body
• The exposure of the Council to adverse publicity or actual or potential monetary loss through any compromise of security
• Any person who knows of, or suspects a breach of the Council’s Information Security Policies must report the facts immediately to the IT Security Analyst or Senior Management, failure to do so will be treated as non-compliance to the Information Security Policy
• Violation or non-compliance with the Council’s Information Security Policy may be treated as gross misconduct.
• Penalties may include:
  o Suspension of system access rights
  o Action in accordance with the Council Disciplinary Code of Conduct
  o Termination of employment or contractual arrangements and civil or criminal prosecution