Acceptable Personal Use of Resources and Assets Policy

<table>
<thead>
<tr>
<th>Document Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>Date Approved</td>
<td>October 2021</td>
</tr>
<tr>
<td>Approved by</td>
<td>Local Governing Body</td>
</tr>
<tr>
<td>Next Review Date</td>
<td>October 2022</td>
</tr>
</tbody>
</table>
Acceptable Personal Use of Resources and Assets
Policy

Explaining what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use

Policy points are numbered. The numbering corresponds to explanations of ‘why?’ and ‘how?’ for each point further down the page.

What must I do?

1. **MUST NOT**: You must not use our facilities to undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material.
2. **MUST NOT**: Personal use must not interfere with your productivity and how you carry out your duties.
3. **MUST NOT**: Personal use must not reflect adversely on our reputation.
4. **MUST**: You must use our facilities economically; your personal use must not create extra costs for us.
5. **MUST NOT**: You must not do anything that would compromise the security of the information held by us, such as downloading/spreading any harmful virus/program or disabling or changing standard security settings.
6. **MUST NOT**: You must not use browsers or access/attempt to access sites that are knowingly unacceptable, even if this is in your own time
7. **MUST NOT**: You must not send or forward chain, joke or spam emails.
8. **MUST NOT**: You must not leave personal-use websites open or minimised on your screen even if this is in your own time when you are not actively viewing/using them.
9. **MUST NOT**: You must not use the Organisation’s facilities for commercial purposes not approved by us or for personal financial gain.
10. **MUST NOT**: You must not use your access rights or identity as an employee to mislead another person for personal gain or in any other way which is inconsistent with your role.
11. **MUST NOT**: You must not disclose (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
12. **MUST NOT**: When you print, photocopy, scan or fax official-sensitive information, you must not leave the information unattended.
13. **MUST NOT**: You must not connect any equipment to our IT network that has not been approved.
14. **MUST NOT**: You must not make personal use of the information available to you that is not available to the public.
Why must I do it?

1. ALL: To ensure we use our IT and other facilities resources effectively, making sure that our reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes.

How must I do it?

1. By complying with the points of this policy.
2. You must only make personal use of our IT facilities outside of time you are recording or is designated as your ‘working hours’.
3. By complying with the points of this policy.
4. By checking with your manager or where you have any uncertainty over what is appropriate.
5. IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
6. By taking care over the sites you are about to open, including reading search report information before opening.
7. By deleting such items if you receive them.
8. Closing websites when you are not actively using them.
9. By checking with your manager where you have any uncertainty over what is appropriate.
10. By checking with your manager where you have any uncertainty over what is appropriate.
11. If you are not sure if you are authorised to disclose information, speak with your manager in the first instance.
12. If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.
13. Check that equipment has been authorised for use by the ICT Technical Department before insertion/ connection.
14. If you wish to utilise Organisation data in a personal capacity, you must make a formal request for information to the Organisation.
What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Gülin Farrance.

References

- Data Protection Act 1998 (to May 25th 2018)
- General Data Protection Regulations (from 25th May 2018)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.