Runwell Community
Primary School

Acceptable Personal Use of Resources and Assets Policy

May 2018 (Review May 2019)

Acceptable Personal Use of Resources and Assets Policy

This policy aims 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 outcome. It sets out what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use and is applicable to ALL Staff Members, Governors and Volunteers.

Policy Requirements

1. You **must** use our facilities economically; your personal use must not create extra costs for us. Where you have any uncertainty over what is considered appropriate you must check with your manager or a member of the Senior Leadership Team.

2. You **must** only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours' Personal use must not interfere with your productivity and how you carry out your duties or reflect adversely on our reputation.

3. You **must** delete any chain, joke or spam emails from your mailbox on receipt and under no circumstances send or forward these, even to your personal email address.

4. You **must** ensure that any official-sensitive information that is printed, photocopied, scanned or faxed is not left unattended. If you are faxing information externally, always ensure 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.

5. Photos of Children or Staff should only be taken for school purposes and when using Personal devices to take pictures of children or staff involved in activities you **must** ensure that these are deleted prior to leaving the premises each day. Even after initial deletion you must access your recently deleted folders and ensure the images are deleted permanently.

6. You **must** check that equipment has been tagged or marked as an accepted and managed device before insertion/ connection to our IT network. Do not connect any equipment that has not been approved.

7. 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 or any material that could be perceived to be offensive. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material.

8. You **must not** leave personal-use websites open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them.

9. You **must not** use browsers or access/ attempt to access sites that are knowingly unacceptable, even if this is in your own time.

10. You **must not** use the Organisation's facilities for commercial purposes not approved by us or for personal financial gain. Where you are uncertain if the nature of your activity requires approval you must check with your line manager or a member of the Senior Leadership Team.

11. 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.

12. 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. Where you are uncertain you must check with your line manager or a member of the Senior Leadership Team.

13. You **must not** do anything that could compromise the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings. Our IT controls should prevent your ability to download anything harmful, but if in doubt, contact your line manager or a member of the Senior Leadership Team.

14. You **must not** make personal use of the information available to you that is not available to the public. 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 the Headteacher.

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.