BEAUCHAMPS HIGH SCHOOL

Beauchamps Drive, Wickford, SS11 8LY
Headteacher: Mathew Harper BA Hons, NPQH

Acceptable Personal Use of Resources and Assets Policy

School Policy/Procedure No: 69

Adopted/Last Reviewed: October 2020 *Last Amended: October 2020* *Next Review: October 2021*

In accordance with the General Data Protection Act 2018, Beauchamps High School has a duty to ensure that all IT and other resources are used effectively, making sure that the school's reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes.

The following guidance outlines what users of the school's resources and assets must or must not do:

Users MUST:	**How :**
1. Use our facilities **economically**; users' personal use must not create extra costs for the school	Check with management where there is any uncertainty over what is appropriate
2. Only use the approved, **secure e-mail** system(s) for any school business	When stakeholders are not in school, Office 365 should only be used when accessing the school's secure e-mail system(s) or a device linked to the school's email account. The use of phones is acceptable as long as they linked to the school email account and they have a passcode applied.
3. Ensure that **all removable devices and laptops** that store student data are **encrypted.**	By checking that your device has encryption turned on. If in doubt contact Network Support so they can encrypt the device.
4. Ensure that they are aware of their surroundings when accessing school data on personal devices.	By checking that no unauthorised persons can view personal devices that are used to view school information.

Users MUST NOT:	**How:**
5. Use the school's 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	By complying with the points of this policy
6. Personal use must not interfere with employees/students' **productivity** and how they carry out their duties	Users must only make use of the school's IT facilities outside of time you are recording as or is designated as your 'working hours' (this applies to staff and students)

7. Personal use must not reflect adversely on the school's **reputation**	By complying with the points of this policy
8. 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	By closing websites when you are not actively using them

Users MUST NOT:	**How:**
9. Use browsers or access/attempt to access sites that are knowingly **unacceptable**, even if this is in employees' own time.	By taking care over the sites you are about to open, including reading search report information before opening
10. **Send or forward** chain, joke or spam emails	By deleting such items if you receive them
11. Use the school's facilities for **commercial purposes** not approved by us or for personal financial gain	By checking with management where there is any uncertainty over what is appropriate
12. Use access rights or identity as an employee/student to access sites that are knowingly **unacceptable**, even if this is in users' own time	By checking with management where there is any uncertainty over what is appropriate
13. Disclose (in writing, speech or electronically) information held by the school unless you are authorised to do so, and the recipients are authorised to receive it	If you are unsure if you are authorised to disclose information, speak to management in the first instance
14. When users print, photocopy, scan or fax official sensitive information, they must not leave the information **unattended**	If you are faxing information outside your immediate office/work area, 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
15. **Connect** any equipment to the school's IT wired network that has not been approved	By checking that equipment has been tagged or marked as an accepted and managed device before insertion/connection
16. Connect any personal equipment to the school's wireless network if it does not have up to date virus protection.	By checking that the device being connected has an up to date virus checker and it is using the most recent virus definitions. If in doubt contact Network Support in the first instance.
17. Do anything that would **compromise** the security of the information held by the school, such as downloading/ spreading any harmful virus/program or disabling or changing standard security settings	IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
18. Make personal use of the information available to you that is not available to the **public**	If you wish to utilise school data in a personal capacity, you must make a formal request for information to the school.

Acceptable Use Agreement:

All users of IT and other resources belonging to the school are required to sign an Acceptable Use Agreement / ICT Charter when they start the school.

Use of Social Media:

Relevant stakeholders will abide by the conditions of use of Social Media as outlined in the Acceptable Use Agreement/ICT Charter (see below).

Actions which are in breach of the policy:

If users believe they have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, they should raise a formal request by contacting the school's GDPR Champion (Mr T Kidman).

Policy breaches:

The school monitors all use of the Internet and other technologies by relevant stakeholders, and monitoring information can be made available, on request, to Line Managers or the Headteacher.

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 (for employees) or exclusion (for students), or in legal action being taken against you.

Note: All data on Acceptable Personal Use of Resources and Assets stored in school is only shared in accordance with the school's Privacy Notice