Hive Bradford

Acceptable use of IT

Last adopted: October 2025	Review: 3 years	Review due: October 2028

Key principles

This policy covers the acceptable and safe use of computers, laptops, tablets, mobile phones and any other IT on Hive premises or during Hive activities at other premises.

Acceptable use of IT

- You must not access, produce, display, distribute, edit or record sexually or racially offensive material. Accessing such material is a very serious matter, which may be reported to the police.
- You must not access or download any illegal material, including material that is inherently illegal, or the illegal downloading of music, video or software.
- You must not access, produce, display, distribute, edit or record any material that endorses illegal, violent or abusive behaviour.
- You must not use the Internet or phone network to harass, abuse, offend or threaten others. Care should be taken not to cause offence unknowingly.
- Hive's facilities must not be used for political campaigning or the promotion of political views.
- Peer-to-peer file sharing (eg. BitTorrent), is not permitted.

If you are aware of breaches of this policy or are subject to online abuse you should report it to a member of staff.

Safe use of IT equipment

Prolonged use of display screen equipment can be damaging to eyesight and you should take regular breaks. Taking short breaks often is better than taking longer breaks less often, for example a 5-10 minute break every hour.

Do not consume food or drinks near IT equipment, where spillages could cause damage.

Do not use equipment with frayed or exposed wires. Report the equipment to the IT lead and take it out of use (labelling it clearly) until it can be repaired or replaced.

No IT equipment should be dismantled except by a suitably experienced or trained person and with the authorisation of the IT lead.

You must not install software to any equipment provided by Hive without permission from the IT lead.

If you are given Hive login details, you must not disclose or share them with anybody else, or allow anybody else to log in using them.

Key contacts

IT Lead: Ben Clymo

Appendix 1: Copyright

UK copyright law automatically protects original literary, dramatic, musical and artistic work (including illustration and photography), original non-literary written work (including software, web content and databases), sound / music / film / television recordings, broadcasts, and the layout of published editions of written, dramatic and musical works.

Work may be marked with the copyright symbol (©), author and date, but material is still automatically protected even without that. No registration of copyright is required.

Copyright ownership generally rests with the person who created the work. However, if the work was created as part of employment (or on a freelance basis where it is specified in the freelance contract), then the copyright will rest with the employing organisation.

You must have the permission of the copyright owner to re-use or adapt any copyrighted material, or to use copyrighted material in anything you publish (which simply means making available publicly in any form, including posting on social media or a website, or displaying publicly). This includes re-using text from websites, or downloading images from the Internet. There are sources of royalty-free images where permission has been granted by the copyright holder to use the images, but this will not apply to the vast majority of images found on websites or via a web search.

You should be aware that it is increasingly common for larger copyright holders to use image recognition software to trawl the internet for their copyrighted images: this could quite easily pick up a seemingly obscure social media post or little-known website that has only been viewed by a handful of people, and potential penalties can be quite severe.

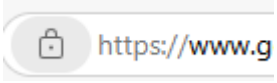
Although there are certain very specific ‘fair use’ rules, any use of copyrighted material, no matter how small, could potentially lead to legal action. If you want to publish an extract or quote, the best guideline is to seek permission before using. You should always acknowledge and link to the original source of any quoted material or extracts.

Appendix 2: Safe use of the Internet

The Internet is a really useful tool, but there are a number of risks associated with going online including malware, phishing (obtaining personal or financial information, potentially using it for ID theft), fraud (including fake websites), copyright infringement and exposure to inappropriate content

To protect yourself online:

- use your instincts and common sense
- be careful revealing personal information: particularly financial information or passwords, but also anything that could be pieced together to impersonate you (eg. birthday, age or address), or that is commonly used in security questions (eg. first school, birthplace, children's or pets' names)
- check for signs that a website is for a legitimate organisation such as listing a verifiable physical address, a phone number (particularly a landline), or an official registration such as a company number, charity number or trade body registration: check that the details given for the entry on the registration body match those on the website
- it is very easy to set up a spoof website that looks very similar to the genuine one, and direct people to it via spam emails or social media posts: be alert for signs that a site is a copy, such as spelling mistakes, a site 'not looking quite right', poor quality images or other warning signs
- check that a website's address seems to be genuine by looking for subtle misspellings, extra words, characters or numbers, or a different name to that of the business: the most important part is that immediately before the top level domain (eg. immediately before .com, .co.uk, .org, .net):
    - **mybusiness**.com – likely genuine
    - **mybusiness**.com /store/nk234oudsflisd/product/ - likely genuine
    - store.**mybusiness**.com – likely genuine
    - store.**mybusiness-payments**.com – likely not genuine
    - **mybusines**.com – likely not genuine
    - **nk234oudsflisd**.com /mybusiness – likely not genuine
    - mybusiness.**nk234oudsflisd**.com – likely not genuine
- hover the pointer over a link to see a preview of the address it leads to in the bottom left or right of the screen – this may be different to the text displayed on the page (and that is a warning sign)
- do not enter any personal information (including financial) into a website, or log in to site, unless it has a security padlock and https:// before the address of the page in the address bar at the top



- beware of being unexpectedly asked to log in – don't enter login details unless you were trying to log into a site, and are sure it is the genuine site and not an impersonation
- offers or deals that seem too good to be true probably are.

More information can be found on the Get Safe Online website at getsafeonline.org/personal/articles/safe-internet-use.