Harwich and Dovercourt High School

Acceptable Use Policy

Document Detail	
Category:	Staff Related / Student Related
Authorised by:	Local Governance Committee
Sponsor:	James Loten
Author:	Mr James Loten
Version:	6
Status:	Approved
Issue Date:	December 2021
Next Review Date:	December 2022

Ownership and Control

History

Version	Author	Dated	Status	Details
1	Kd	23/10/14	Approved	Approved by the Student and Curriculum Committee 22 October 2014
2	Kd	11/05/2016	Approved	Re-approved 11 May 2016
3	Kd	14/06/2017	Approved	Reviewed and approved by the Local Governing Board 14 June 2017
4	MHI	Nov 2019	Approved	Approved by LGB 7th November 2019.
5	MHI	Nov 2020	Approved	Approved by LGC 5th Nov 2020
6	JLO	Dec 2021	Approved	Approved by LGC 7th December

Intended Audience

Intended Audience	Intended Method of Distribution
Staff / Students	Shared Staff Google Drive, Website

Harwich and Dovercourt High School - Computer Network Acceptable Use Policy

If you have any questions about the policy, please contact the IT Support Team in the first instance.

The School assumes the honesty and integrity of its IT users. Facilities are provided in as unrestricted manner as is feasible in order to offer the best possible quality of service.

It is the user's responsibility to ensure that they comply with the policy. The latest version may be seen on the School Website and is in addition to the school's Code of Conduct Policy.

All staff and students will be expected to sign an agreement to abide by the policy.

Refusal to follow any of this policy when pointed out by a member of staff will be treated as any other refusal to follow an instruction, in line with the School's Behaviour for Learning Policy or Code of Conduct.

1. General Policy

The user agrees not to:

Upload, download, post, email or otherwise transmit or store any content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, lewd, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethnically or otherwise objectionable.

Impersonate any person or entity, or falsely state or misrepresent affiliation with a person or entity including the forging of headers or to otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the School services.

Upload, download, post, email or otherwise transmit or store any content that the user does not have the right to transmit.

Upload, download, post, email or otherwise transmit or store any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party.

Upload, download, post, email or otherwise transmit or store any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" etc. except when directly resulting from curriculum work.

Upload, download, post, email or otherwise transmit or store any material that contains software viruses or any other computer code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software, hardware or telecommunications equipment.

Interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.

Collect or store personal information about others without direct reference to The Data Protection Act.

Use the School's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes unless as part of a curriculum project.

Visit or use any online messaging service, "chat site", web-based email or discussion forum not supplied or authorised by the School.

Store or use any software not specifically installed on the computer network by a member of the IT Support Team.

Visit, use, download, or store any game, either application or browser-based, without permission of a supervising teacher, and only for educational purposes.

The School reserves the right to refer any breach of this policy to the respective Mentor / Tutor / Head of Department and / or member of the Leadership Team. This may result in the suspension of any or all parts of the services provided.

2. Network Services

This comprises of access to desktops, laptops, tablets (PC or Mac based) and Chromecasts\Apple TV's in the various classrooms, labs or other areas for all users, and for staff additional access in departmental offices for the purposes of School Administration.

Storage of files for all users is available on the School network.

All users shall have complete access to any files they have created, except where ownership / authorship is in question. This is then referred to the relevant Mentor / Tutor / Member of the Leadership Team.

Each user shall have a unique username and password. The password must not be divulged to any other user or any third parties outside of the School.

3. Internet Services

Each User shall have access to the Internet via the School's Proxy Server. The Proxy Server will filter any unwarranted materials and be updated regularly to maintain this high level of filtering.

Any user repeatedly attempting to access such material will have their account locked and it will not be reopened until they have discussed the matter with a member of the Leadership Team.

The School does not pre-screen content viewed by users, but relies on the filtering software. Should any site or content be discovered which does not comply to the General Policy it will be added immediately to the deny list. Users should report offending material to IT Support by supplying the complete website address.

Whilst the school makes every effort to filter material as defined in the Code of Conduct, the school cannot be held liable for any failure to filter such material due to the nature and proliferation of such sites on the internet.

There are systems in place to monitor all network usage and as such there is no expectation of privacy on the school's network regarding access. This extends to the use of school computing property used away from the school site. There are also systems in place to monitor activity that may compromise the school and its stakeholders within cyberspace, including media and social media.

4. Mail Services

If a user sends an email that contains content as defined in the Code of Conduct Policy or Behaviour for Learning Policy, their account shall be locked and not released until they the school has received authorisation from a parent or guardian and then only in consultation with a member of the leadership team, or their line manager and then only in consultation with the Headteacher.

If a user repeatedly sends material as defined in the policies above the matter will be referred to the Headteacher

Any user who receives unsolicited mail can inform the IT Manager who will endeavour to trace the originator and report them to their Service Provider.

Likewise, if any user is found to be sending unsolicited emails, to other users within the school, or to external accounts, the matter will be referred to the Headteacher.

The standard disclaimer should be attached to all outgoing mail and should not be modified in any way; this is to protect both the interests of the school and the individual.

Users' email can be monitored by IT support at the request of the Headteacher, Governing Body or other legal agencies.

There are systems in place to monitor all email usage and as such there is no expectation of privacy on the school's network regarding email services.

5. Security

Each User will be given a unique username and password that will allow them to access their account.

The username and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason. If a user is found using the username and password of another user their services may be suspended and immediately referred to the Headteacher.

The only programs that may be used within the School are those agreed on by the IT Manager and / or Leadership Team and installed by a member of IT Support. The introduction of programs (including any software containing viruses or used to disrupt any part of the Network, or connected networks) onto the network is not tolerated and will be treated as intentional damage or an attempt to cause damage to School property.
All information about staff and students will be dealt with in compliance the Data Protection Act and only given to authorised agencies. Staff and students agree to abide by the Data Protection Policy.

The School reserves the right to monitor all traffic on the network and school computing property including but not limited to user's individual saves areas, either manually or through automated software, to ensure policy compliance and to aid in resolving any issues.

While the school takes every precaution to ensure adequate backups of all data stored on its servers, users should be mindful of ensuring they have taken appropriate steps to safeguard their own work. This could be accomplished by copying files to USB drives or using other appropriate methods.

6. Treatment of Equipment

IT Support will endeavour to ensure all equipment is in working order, should any user find that a piece of equipment does not work correctly they are to report it to a member of IT Support and not attempt to repair it themselves.

Any user who causes damage directly or indirectly intentionally, through neglect or through any other actions to any equipment may be refused the right to further use of the equipment and may be asked to cover costs towards any repairs or replacements.

Appendix 1 - Acceptable Use Agreement Form

At Harwich and Dovercourt High School students and teachers work together to form a challenging learning environment, create mutual respect, and engender responsible attitudes to each other, to work and to property is the foundation of the School's culture.

The computer and IT system at Harwich and Dovercourt High School is the property of the School and is a resource shared by all students and staff. Computer facilities, including mobile units, are made available to further student education and to staff to enhance their professional activities, including teaching, research, administration and management.

The School's Acceptable Use Policy has been drawn up to protect all parties – the students, the staff and the School. A copy of the School's Acceptable Use Policy is available on the Staff Shared Drive, in the Policies folder. The Acceptable Use Policy is in addition to the school's Code of Conduct.

Key Points:

The School reserves the right to examine or delete any files, including emails, that may be held on its computer system; and to monitor or to restrict access to any Internet sites visited.

Students and Staff using the School's computer system should sign a copy of the Acceptable Use Statement and return it to their tutor or to the IT Operations Manager as appropriate, or to agree to the Statement via the dialogue box when logging into the system.

All Internet activity should be appropriate to staff professional activity or student education

- Access to the School servers and the Internet should only be made via the user's authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the School IT systems, or activity that attacks or corrupts other systems is forbidden
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received

Copyright of materials must be respected

- Use for personal financial gain, gambling or political purposes is forbidden
- Use of the network to access inappropriate material is forbidden
- Video, audio or photographic recording of staff or students whilst on School property, to be used outside of the School or for activities other than those authorised by the School is forbidden

PLEASE SIGN AND DATE BELOW:

Name (Please Print):

Tutor Group: (students only)

Signed: Date: