DAWLISH COLLEGE

Student ICT Acceptable Use Policy

Applicable to all students at Dawlish College

1 - Acceptable Use Policy for the IT Network

Contents

1.1 Purpose

The purpose of this policy is to outline the acceptable use of the Dawlish College IT network. This policy also applies to remote access of the college IT network and the use of ICT systems managed by the college, including E-Praise and any Virtual Learning Environment (VLE).

Separate acceptable use policies are available for E-mail and the Internet and users of these services are required to adhere to these and any other relevant college policies.

Inappropriate use of the college IT network may expose the college to unnecessary risks including virus attacks, compromise of network systems and services, financial and legal issues. The aim of this policy is to protect both staff and students.

1.2 Eligibility

All students will be issued with a logon to access the college IT network.

Every user who is issued with a network logon will be asked to sign to acknowledge that they have read, understood and will comply with this policy.

1.3 Acceptable use

Individuals are responsible for their use of the college computer IT network. The college IT network is provided for use by students to support their education. Users are expected to respect the property of others, in particular data held on college systems.

Users must take all reasonable precautions to prevent other persons from using their equipment to gain access to internal or external systems to which they have not explicitly been granted access.

Users should be aware that use of the college IT network and the contents of home directories and workgroups is monitored. No expectation of privacy should be taken with regard to any files. In accordance with UK Law, a designated authority may, on behalf of the college, authorise the monitoring of files.

1.4 Unacceptable use

The college IT network must not be used for any of the following:

- the creation or storage, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- the creation or storage of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- the creation or storage of defamatory material
- the creation or storage of material such that this infringes copyright or the intellectual property rights of another person
- deliberate activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time and the effort of staff involved in the support of the IT systems
    - corrupting or destroying other users' data
    - violating the privacy of other users
    - disrupting the work of other users
    - using ICT facilities in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
    - continuing to use an item of networking software or hardware after being requested that use cease because it is causing disruption to the correct functioning of the network
    - other misuse of networked resources as identified by the network administrator, such as the introduction of "viruses"

Users must in no way attempt to gain access to internal or external systems to which they have not been granted access. This includes browsing the network drives without authorisation.

Users must never allow another person to use their logon or use the logon of another person. Users may be held responsible for the actions of, and any consequences of, any other individual using their logon.

Users must not in any way cause any form of damage to the college's computing facilities or any of the accommodation or services associated with them.

Users must not consume food or drink into rooms that contain ICT equipment.

Users must not abuse printing resources (see section 1.9).

1.5 Hardware

Do not move computer equipment or rearrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.).

No internal or external devices e.g. peripheral equipment other than USB memory devices should be added or removed from computer equipment without consulting IT Support.

Use of personal equipment

Users are reminded that the college's ICT Acceptable Use Policies apply to the use of personal devices whilst connected to the college wireless network.

1.6 Software

Software may only be used for the purposes of learning, research and personal educational development or for other purposes as defined in the licensing agreement. Software may only be used on computer equipment covered by that agreement.

Users must not download or install software.

1.7 File management

It is the responsibility of each user to ensure that they regularly delete files that are no longer required. Limits are imposed on the amount of file storage space made available to individual users. These limits are reviewed on a regular basis by college management/IT Support.

IT Support will monitor the size of individual files stored on a network drives (individual home directories and workgroups) as large files, particularly images or audio and video, use up disc space very quickly and can bring the network to a standstill.

Users are not permitted to store any archive (*.zip, *.rar) or executable files (*exe. *.bat, *.msi, *.scr or *.com) on the college network without authorisation of a member of the IT department (some executables files are created by software currently used for some of the ICT curriculum). IT Support will perform regular checks for these files and where files or software of this type are found these will be deleted or access to these files will be removed and further action may follow. Students are not permitted to run executable files from removable media.

1.8 Security

Passwords

Access to the college IT network is controlled by username and password.

Users and/or IT Support may be required to change passwords if IT Support consider there is a possible security risk.

Passwords must not be divulged to third parties and users must take all reasonable precautions to ensure that their password remains confidential. In particular, passwords must never be written down.

New accounts will be set up with a temporary password and will remain disabled until the user contacts IT Support.

If a temporary password is issued for any reason the user must log on and change the password immediately; failure to do so will create a security risk.

Anti-virus

Users must not interfere with the operation of the anti-virus software or change its configuration.

Transferring files

Users needing to transfer files onto the college network from removable media other than USB memory devices e.g. CD, mobile phone, floppy drives should contact IT Support.

Alternatively, users who have access to email may transfer files electronically in accordance with section 3.5 of the Acceptable Use Policy for E-mail.

1.9 Printing

Student printing (both monochrome and colour) is controlled by a release system managed by staff, who can elect to print a document, cancel it or leave it in the print queue. Documents that have not been printed within a set period of time after submission are automatically deleted.

Each time a document is sent to the printer it must be assigned to a subject area. A report listed all documents printed for each subject area (specifying the user, number of pages etc.) is generated on a monthly basis and issued to the relevant member of staff.

A user's ability to print may be withdrawn if this is misused. Examples of misuse include:

- wasting resources e.g. wasting paper by printing multiple copies of the same document, wasting toner by printing documents with dark backgrounds
- printing 'junk' i.e. clipart pictures with captions
- printing anything that is deemed to be offensive
- printing large amounts of documents for personal use i.e. not college work

1.10 Termination of accounts

Computing accounts will be terminated when users cease to be a member of the college.

Files will be archived and removed from the network drives. In the event of the student transferring to another college arrangements should be made with IT Support for the appropriate files to be transferred.

1.11 Personal/recreational use

The provision of the college IT equipment is primarily intended for the business of Dawlish College. Limited personal use is also permitted, provided this does not interfere with learning or the operation of the network and complies with all college Acceptable Use Policies.

1.12 Monitoring

Users should be aware that use of the IT network, including the contents of home directories, virus activity reports and printing logs, is monitored in accordance with this policy and the college's Policy on Monitoring and Interception.

2 - Acceptable Use Policy for the Internet

Contents

2.1 Purpose

The purpose of this policy is to outline the acceptable use of the Internet by Dawlish College students. As access to the Internet is only available via the college IT network, this document must be read in conjunction with the college's Acceptable Use Policy for the IT Network.

Inappropriate use of the Internet may expose the college to unnecessary risks including virus attacks, compromise of network systems and services, financial and legal issues. The aim of this policy is to protect both staff and students.

2.2 Eligibility

Every user who is entitled to Internet access will be asked to sign to acknowledge that they have read, understood and will comply with this policy. A signature will also be required from a parent/guardian/carer and Internet access will not be granted until this has been received.

2.3 Acceptable use

Use of the Internet by Dawlish College students is permitted and encouraged where such use supports learning.

All users must use a filtered Internet service in accordance with Devon County Council policy.

Users must be aware that the Internet is inherently insecure and personal information must never be disclosed.

One of the main benefits of the Internet is the access which it gives to large amounts of information which is often more up-to-date than in traditional sources like libraries. Unfortunately, as the Internet is uncontrolled, some of this information is less accurate than it may appear and users must be aware of the risk of obtaining and using such unregulated information.

Although the college has anti-virus defences in place, great care should be taken when using the Internet. IT Support should be informed immediately if any suspicion of virus infection arises.

Downloading / Uploading

The copyright and intellectual property rights of material accessed using school systems must be respected. Downloading of all copyrighted material from the Internet without the permission of the copyright holder is illegal under the Copyright, Designs and Patents Act (1988). Any copying without permission, including electronic copying, is prohibited. In addition, the storage and distribution of copyrighted files may also make the individual liable to prosecution.

Users must not upload or transfer files via the Internet using FTP.

In accordance with the college's Acceptable Use of the IT Network policy, no software may be downloaded or installed from the Internet.

2.4 Unacceptable use

Users must in no way access or attempt to access material that is illegal, defamatory, obscene or potentially offensive.

Users must not use any college equipment to host websites or use remote hosting.

The use of chatrooms is not permitted nor is submitting posts to bulletin boards.

Users shall not compromise any aspect of network security, such as in use of peer-to-peer access for file sharing e.g. KaZaa or participation in on-line gaming.

Any personal use that disrupts or prevents learning will not be allowed.

Offensive material

Users must not access any material which may be considered to be libellous, pornographic, sexually explicit, or which include hostile material relating to gender, sex, race, sexual orientation, religious or political convictions or disability, or incitement of hatred, violence or any illegal activity.

Although a filtering service is used by Dawlish College, the Internet is growing so rapidly that it is impossible to prevent all inappropriate access automatically. If a user accidentally accesses material of the type referred to above, or other material which they feel may be considered of an offensive nature, they should inform a member of college staff immediately.

2.5 Monitoring

No expectation of privacy should be taken with regard to Internet use. Users should be aware that Internet use, including virus activity reports, is monitored in accordance with this policy and the college's Policy on Monitoring and Interception.

3 - Acceptable Use Policy for E-mail

Contents

3.1 Purpose

The purpose of this policy is to outline the acceptable use of e-mail by Dawlish College students. As access to e-mail is only available via the college IT network, this document must be read in conjunction with the college's Acceptable Use Policy for the IT Network.

Inappropriate use of e-mail may expose the college to unnecessary risks including virus attacks, compromise of network systems and services, financial and legal issues. The aim of this policy is to protect both staff and students.

3.2 Eligibility

Every user who is entitled to an e-mail address will be asked to sign to acknowledge that they have read, understood and will comply with this policy. A signature will also be required from a parent/guardian/carer and access to e-mail will not be granted until this has been received.

3.3 Acceptable use

Dawlish College provides an e-mail system to support its activities and access to this system is granted to users on this basis.

Users should be aware of current e-mail etiquette and procedures for dealing with spam/unsolicited mail.

Users should be aware that e-mail use and the contents of e-mail folders is monitored. E-mail messages sent and received from the college e-mail system are not private property; they form part of the administrative records of the college and may be inspected at any time. In accordance with UK Law, a designated authority may, on behalf of the college, authorise the monitoring of communications and or access logs.

3.4 Unacceptable use

Users must not start or forward any chain e-mails, jokes, spam, animations etc. Do not forward any e-mails warning about viruses as they are invariably hoaxes. If in doubt, contact IT Support directly for advice.

Users must not distribute or disseminate any images, text or material which might damage, overload, affect, or have the potential to affect, the performance of the college IT network and/or external communications.

Users must not send or forward any material that could be considered to be obscene, suggestive or defamatory or may harass, distress or otherwise offend the recipient. Users must not send or forward any material which may be considered to be libellous, pornographic, sexually explicit, or which includes hostile material relating to gender, sex, race, sexual orientation, religious or political convictions or disability, or incitement of hatred, violence or any illegal activity. Due regard shall be given to the provisions of the Malicious Communications Act 1988 in addition to college guidance in this respect.

Users who open an e-mail containing any material referred to in the paragraph above should inform IT Support. If the e-mail originated from a sender from outside the college who is personally known to the recipient, it is the responsibility of the recipient to delete the e-mail immediately and contact the sender to request that no messages of similar content are received in the future. Failure to do so may result in e-mail facilities being withdrawn.

Users are not permitted to distribute any files that infringe copyright.

Users must not transmit any viruses or malicious code.

Users must not attempt to access the mailbox of another user.

Users must never allow another person to use their e-mail account or use the e-mail account of another person. Users may be held responsible for the actions of, and any consequences of, any other individual using their e-mail account.

Users must not send e-mails purporting to come from another user by forging the e-mail address of the sender (spoofing).

Users must not disclose their college e-mail address to external organisations, as this information may be passed to other organisations generating unsolicited mail.

Users must not use their college e-mail address to sign up to any websites.

Excessive use of the e-mail system for ‘chatting’ to friends will not be allowed.

Any personal use that disrupts learning will not be allowed.

3.5 Attachments (sending & receiving)

Only attachments relating to college work should be sent.

All e-mails sent from or received by the college are scanned for blocked file names and blocked file types by the college's e-mail provider. If the file name or file type of an attachment matches any of the blocked rules then that attachment is replaced with a warning text file and the message is delivered to the recipient. The rules for blocked file names and blocked file types can be obtained by contacting IT Support.

Access to attachments is further restricted by Microsoft Outlook. These restrictions may either deny access to an attachment or prevent users opening the attachment directly from the e-mail (the attachment must be saved before it can be opened). If these restrictions prevent a user from accessing an essential attachment they should contact IT Support.

Attachments should be no bigger than 2Mb in size. This is important, not only to stop the network slowing down but also to ensure that data is transferred efficiently and securely. Files larger than 2Mb should only be sent out by arrangement with IT Support.

3.6 Viruses

All e-mails sent from or received by the college are scanned by the college's e-mail provider for viruses. If a message is found to contain a virus the message is discarded. Neither the sender nor the recipient is informed since most viruses spoof the sender's address. A copy of the message headers is logged in a database together with the identity of the virus detected. This database is maintained by the college's e-mail provider.

Please also refer to the Security section of the Acceptable Use Policy for the College IT Network.

3.7 Mailbox management

Users will be allocated a mailbox of finite capacity. It is the responsibility of each user to ensure that they regularly delete e-mails that are no longer required and to ensure that the Deleted Items folder is emptied. If users fail to manage mailboxes e-mail privileges may be withdrawn.

3.8 Monitoring

No expectation of privacy should be taken with regard to e-mails. Users should be aware that e-mail use, including the contents of e-mail folders, is monitored in accordance with this policy and the college's Policy on Monitoring and Interception.

E-mail messages that have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending e-mail can be identified. This feature will only be used for monitoring purposes and not for retrieving messages that have been deleted accidentally.

4 - Policy for Monitoring and Interception

Contents

4.1 Purpose

As part of the risk-minimisation process, Dawlish College exercises its right to monitor electronic communication and network usage for the purpose of recording evidence of transactions, ensuring regulatory compliance, detection of crime or unauthorised use and to ensure the operation of all systems and services. This is in accordance with the Provisions of the Regulation of Investigatory Powers Act 2000 and guidance from the Data Commissioner.

4.2 Guidelines

Wherever practicable, monitoring shall be conducted by automated means so as to reduce the risk of disclosure of the activities of individuals. Targeted covert surveillance on individuals will only be conducted with the express authorisation of the college management.

College systems automatically record all user account logins and accesses across the college network. These logs are retained for one academic year before being archived. These logs are used for system monitoring and maintenance, auditing or as part of a criminal or disciplinary investigation.

The college maintains the right and ability to carry out detailed inspection of any IT resources, including computers, email and voicemail, and review or delete any data recorded in those systems to ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.

Should any individual have reasonable grounds to suspect that a user has broken college policy on the use of IT they should contact IT Support. Depending upon the severity of the breach, IT Support may refer the matter to the college management team. Upon receiving such a report the college management may authorise the investigation and or monitoring of logs. The result of such an investigation may result in disciplinary proceedings.

IT Support may be required to access files whilst in the process of fixing problem. If any breaches of IT policy are discovered during this process, action will be taken as described above.

Access to home directories will be granted as part of a criminal or disciplinary investigation.

4.3 Actions / Enforcement

When a breach of the college's acceptable use policies is identified:

- action may be taken by IT Support.
- action may be taken by a member of ICT teaching staff.
- action may be taken by college management.

Actions may range from loss of access to network facilities e.g. particular software, printing, Internet access to loss of access to the ICT facilities as a whole and, depending on the severity of the breach, may be temporary or permanent.

IT Support will keep records of breaches of the acceptable use policy.