Dauntsey's School

THE USE AND ABUSE OF TECHNOLOGY POLICY

INTRODUCTION

Scope

This policy has been authorised by the Governors and is addressed to all pupils. It is available to parents on request. The policy relates to the use of

- e-mail
- the internet
- Social networking web sites, for example Facebook
- mobile phones with camera facilities
- other photographic or electronic equipment, including palmtop computers and games' consoles
- Dauntseys.NET

POLICY

Aims

1. The aims of this policy are:

    1.1 to encourage pupils to make good use of the educational opportunities presented by access to the internet and other electronic communication

    1.2 to safeguard and promote the welfare of pupils

    1.3 to minimise the risk of harm to the assets and reputation of the School

E-mail and internet protocol

2. This policy authorises the School Rules and Procedures for use of e-mail and the internet at school and sets out sanctions for their misuse. [The ICT Acceptable Use Policy is attached as Annex A].

Sanctions

3. Where a pupil breaches the School's ICT Acceptable Use Policy, the Governors have authorised the Head Master to apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, temporary or permanent exclusion.

Procedures

4. This Policy authorises the Head Master to implement and enforce procedures dealing with the following:

    4.1 entering into, and maintaining, a filtered service with the School's internet content management company

    4.2 the purchase and upgrading of appropriate software and support, including in relation to virus detection

    4.3 setting up and maintenance of auto signatures for outgoing e-mails

    4.4 training pupils in the use of e-mail and the internet, particularly in the context of this Policy and the ICT Acceptable Use Policy

    4.5 control of physical access to the School's computers

    4.6 supervision and appropriate monitoring of pupils' use of e-mail and access to the internet

The liability of the School

5. Unless negligent under the terms of this Policy, the School accepts no responsibility to the pupil or parents caused by, or arising out of, a pupil's use of e-mail and the internet whilst at school.

6. The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

Social networking web sites

7. Pupils should not access social networking websites when using School computers or personal mobile devices through the network when on School premises (apart from Facebook at the allocated times - see ICT Acceptable use Policy for Pupils).

8. In relation to computer use outside school, pupils will be held personally responsible for all material they have placed on a website and for all material that appears on a website of which they are the account holder.

9. In addition pupils must seek, and receive, the express permission to upload any media material from all those who are involved in it.

10. Pupils who fail to follow these guidelines will be subject to school discipline if the welfare of other pupils, or the culture or reputation of the School, are placed at risk.

11. Permanent exclusion is the likely consequence for any pupil found to be responsible (as explained above) for material on his or her own website, or placed by them on another website, that would be a serious breach of school rules in any other context.

Mr P T Jones
Head of IT Services

Reviewed: September 2022
Next Review: September 2023

Annex A

Dauntsey's School

ICT ACCEPTABLE USE POLICY FOR PUPILS

Dauntsey's enjoys the privilege of a computer system with connection to the global ICT community and misuse of the system can cause significant disruption to the work of other members of the School. All users of the School's ICT facilities are deemed to have agreed with the conditions of the Acceptable Use Policy. This is published on Dauntseys.NET.

The key points of the AUP include:

- Access to the network is only possible with a valid username and password. The username uniquely identifies each individual, who is then personally responsible for all activity that takes place through the use of this username. Passwords must never be disclosed to any other person, either inside or outside School.
- Access to the Internet is both filtered and monitored in order to minimize the potential for harm to individuals by contact with materials that is defamatory, abusive, obscene, indecent, racist, sexist, in breach of copyright or otherwise inappropriate including material that seeks to promulgate terrorist activities and radicalist points of view.
- The use of e-mail and access to the Internet is only permitted once you have received your user name and password.
- During lesson and prep times the use of e-mail and access to the Internet from the School's computers and network should be for educational purposes only. Facilities for personal, social or non-educational use are provided at certain other specified times.
- Users must not:
  - Tamper with any school computing equipment, nor remove it from School.
  - Interfere with, or bypass, the security controls on the computer system.
  - Use technology in a way that causes hurt or harm to another pupil or to a member of staff.
  - Install, or alter, software on any of the School's computers.
  - Write computer viruses or knowingly introduce computer viruses.
  - Use any of the School resources or facilities to assist or support any illegal activity.
  - Knowingly attempt to access and download or upload Internet material that is hurtful, defamatory, abusive, obscene, indecent, racist, sexist, or in breach of copyright, or is

otherwise inappropriate, including material that seeks to promulgate terrorist activities and radicalist points of view.

- Send or store e-mails or attachments containing material that is hurtful, defamatory, abusive, obscene, indecent, racist, sexist, or in breach of copyright, or is otherwise inappropriate, including material that seeks to promulgate terrorist activities and radicalist points of view.
- Publish material about, or on behalf of, the School on the Internet without first seeking authority from the Head of IT Support or a member of the Senior Management Team.
- Make use of any electronic image(s) stored on the School network to create a meme, or other depiction, of another pupil or member of staff.
- Under data protection legislation and laws relating to confidentiality, publish personal details of identifiable individuals, even if accessed inadvertently, on the Internet without first obtaining the subject's permission or the permission of the subject's parent/guardian.
- Cancel or dis-apply the School auto-signature/disclaimer attached to all e-mail messages.
- Send or receive encrypted messages; if such a message is received it must be referred to the ICT Support staff.
- Connect personal computers to the School wired network.
- Make use of any ICT facilities, whether within or outside the School, in a manner which may adversely affect the reputation of the School.
- Attempt to use an alternative means of gaining internet access on the School network in order to view material which is blocked by the School's filtering system.

- Users must:
  - Assume that all material on the Internet is protected by copyright and therefore treat such material appropriately and in accordance with the owner's rights – e.g. pupils must not plagiarize another's original work.
  - Tell IT Support or a Senior Member of Staff immediately if they have accidentally read, downloaded or have been sent inappropriate material, which might be considered to be hurtful, defamatory, abusive, obscene, indecent, racist, sexist in breach of copyright, or otherwise inappropriate, including material that seeks to promulgate terrorist activities and radicalist points of view.
  - Only connect personal computers to the School WiFi having followed the guidance provided by IT Support.
  - Have up-to-date Anti-virus software installed on personal pcs and laptops.
  - Be aware of the appropriate uses of Skype/Microsoft Teams and ensure that, in all instances, they are protected by acting responsibly when using it.

- Users of cameras or mobile phones (with or without camera facilities) must adhere to the following guidelines:

- Using mobile phones or photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether the device is used inside, or outside, School.
- Pupils may only use cameras (or mobile phones with camera facilities) with the express permission of the member of staff in charge of an activity and with the permission of those appearing in the image.
- All pupils must allow a member of Senior Management or their Housemaster or Housemistress access to images stored on mobile phones and/or cameras. If it is believed by such persons that they are inappropriate in terms of being hurtful, defamatory, abusive, obscene, indecent or racist or that they might be used to bully, harass or intimidate others, they must delete images if requested to do so by a member of Senior Management or their Housemaster or Housemistress.
- Posting of photographic material on websites such as YouTube, Facebook, Instagram etc. which, in the reasonable opinion of the Head Master, is considered to be offensive, hurtful to others or potentially damages the reputation of the School is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. This is the position whether the electronic device used belongs to the School or is a separate device operated in the pupil's home or in School.

Users of ICT equipment must be aware of the following points:

1. Individuals will be held personally responsible for all material that they have placed on a website and for all material that appears on a website for which they are the account holder.
2. If the Head Master has reasonable grounds to believe that a pupil's mobile phone, camera or personal laptop contains image(s), text message(s) or other material that may constitute evidence of criminal activity, he may hand the phone, camera or laptop to the police for examination.
3. Use of cameras, mobile phones with camera facilities or laptop computers in breach of this policy may result in confiscation of the equipment for a period of time deemed reasonable by the Head Master, and the pupil may be permanently prevented from bringing a camera, mobile phone or laptop onto School premises in future.
4. A pupil must not expect to keep his/her place in the School if he/she is responsible (in the sense explained above) for material on his/her own, or another, website that would be a serious breach of School rules in any other context.
5. Any misconduct, as outlined in this document, outside School will be liable to School discipline if the welfare of another pupil or the culture or the reputation of the School is placed at risk.
6. Failure by a pupil to abide by these guidelines may result in legal action being taken against them by any individuals, entities or organisations who consider that they have been slandered or defamed.
7. For their own protection and that of others, pupil use of e-mail, Internet and any Dauntsey owned laptop\workstation is monitored by the School and may be made available to their teachers. It is important to remember that once an e-mail, or anything downloaded from the Internet, has been deleted, it can still be traced on the system.
8. An individual immediately loses control of any image or text that is sent to others, or placed on the Internet, since it can be copied, altered and retained.

9. Online contacts may lie about their identity. Pupils must know that information on the web can be unreliable and be very cautious about who and what is believed.

The sanctions for any pupil misusing the facilities will depend upon the nature of the incident. They will range between:

- a Saturday evening Detention plus the possible withdrawal of unsupervised access to the network for up to one week and
- temporary or permanent exclusion at the Head Master's discretion.

In addition, a pupil (or their parents) may also be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the School as a result of the breach.

Individuals must be aware that in breaching any of the above guidelines they may also be acting illegally.

Mr P Jones
Head of IT Services

Reviewed: September 2022
Next Review: September 2023