

# DOWNSIDE

---

# SCHOOL

## E-SAFETY POLICY incorporating THE ACCEPTABLE USE PROVISIONS (AUP)

### **Aims of the Policy**

The aims of the e-safety policy are:

- To promote the welfare and safeguarding of pupils and staff at Downside School.
- To ensure that pupils are ICT literate and can use the facilities to ensure that their educational provision is enhanced to the maximum.
- To promote responsible and effective use of electronic communication (including the use of the Internet and mobile phone technology).
- To educate pupils and staff about the risks and responsibilities involved in the use of new technology.
- To raise awareness of and counter instances of cyber bullying.

### **Management of the Policy**

The designated Child Protection Person will serve as the e-Safety Coordinator. The e-Safety Policy and its implementation will be reviewed annually. This policy should be read in conjunction with the following School policies:

- The Child Protection Policy;
- The Anti-Bullying Policy;
- Photographic Policy;
- The Rules and Regulations.

The following measures are in place to support this policy:

- The induction of new pupils and staff;
- The PSHCE and ICT programme;
- Guidance during any academic lesson about use of the internet;
- Specific guidance to exam classes regarding plagiarism.

## **Access to the Internet**

Access to the Internet for pupils and staff is governed by the Acceptable Use Provisions (AUP) (see below), which lays down the framework within which the School network can be accessed, and includes clear guidelines about staff and pupil behaviour in relation to the Internet and the use of the School network.

Downside School will do all it can to monitor access to the internet via the School network. Access to the School Internet has been designed expressly for the use of pupils and includes filtering appropriate to the age of the pupils. The security of the School information systems will be reviewed regularly and virus protection is updated on a regular basis.

The School will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law, and the pupils will be taught to be critically aware of the materials they read. They will also be taught to acknowledge the source of information used.

Pupils and staff are granted access to the internet by agreeing to the terms of the AUP. Any student or member of staff who breaches these terms may have access to the internet withdrawn.

## **E-Mail**

Pupils and staff are inducted into the appropriate use of e-mail and there is clear guidance in the AUP about what is and is not acceptable in terms of e-mail communication. Any inappropriate e-mail must be reported to the ICT Manager, who will immediately inform the Deputy Head Master, and, where appropriate, the relevant HsM.

## **Social Networking Sites**

Pupils are advised never to give out personal details of any kind which may identify them and/or their location. No information may be posted which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute. Members of staff are advised not to run social network spaces for pupils' use on a personal basis and are advised not to allow any current student to be their 'friend' on such a site. Pupils and members of staff are advised always to keep their profile private.

## **Cyber Bullying**

Technology can be used to bully for reasons such as race, religion, sexuality, disability and can be via text message, instant-messenger services and social networking sites, e-mail and images or videos posted on the Internet or spread via mobile phone

The Internet and social networking sites must not be used to hurt, humiliate, slander or defame another person. The same sanctions will apply to incidents of cyber-bullying as would apply to any other form of bullying.

Pupils are made aware that actions in this regard undertaken outside School may also contravene School policy and be subject to School sanctions in the first instance.

### **Mobile Communications and Emerging Technologies**

Pupils and staff are made aware that the guidelines which apply to the use of the School network also apply to any handheld communication device which is brought onto the School site. Nothing which is inappropriate or potentially illegal should be downloaded or saved onto these devices and all should be aware of the possible criminal offence of transmitting such material.

### **Complaints about Pupils**

Complaints of serious Internet misuse will be reported to the Deputy Head Master and will be handled by the Director of Pastoral Care. All incidents of serious Internet misuse must be recorded and passed on to the HsM.

## ACCEPTABLE ICT USE PROVISIONS (AUP) for Downside School Pupils and Employees

These provisions outline the terms and conditions on which Downside School pupils and employees are given access to the network system.

You (and, in the case of a pupil, your parents) have agreed that you will use the Internet, email and other ICT facilities at school in a safe and responsible way and observe all the restrictions explained to you by the school by signing the Acceptable Use Policy Permission Form. If you have not done so, then you may not use the computer system.

Appropriate disciplinary measures will be taken against any user who does not comply with the Acceptable Use Provisions and the Rules for Use of the ICT Centres that are published from time to time and that are displayed in each ICT Room.

The following Acts of Parliament could have relevance to activities possibly carried out using the school's ICT facilities:

Computer Misuse Act 1990  
Copyright, Design and Patents Act 1988  
Data Protection Act 1998  
Defamation Act 1996

Obscene Publications Act 1959  
Protection of Children Act 1978  
Terrorism Act 2000  
Various Discrimination Acts

### **The Computer Network**

The school gives no guarantee that the functions or the services provided by or through the school system will be error-free or without defect. The school will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The school will not be responsible for financial obligations arising through the unauthorised use of the system.

The computer network is an important educational tool used both for administrative and teaching purposes.

Pupils will be taught how to use the network within the curriculum. In addition, pupils have access to the network during non-timetabled learning time for legitimate school work such as research purposes, coursework writing etc., provided ICT rooms are not in use for other teaching, Please see the published rules for more information. Pupils are also encouraged to make use of the school network at recreational times provided that priority is always given to those who may wish to do school work and that pupils use it under the terms of this Acceptable Use Provisions

Employees may have access to the network at any time subject to any restrictions contained in this Acceptable Use Policy or any that may be published by the Head Master from time to time and provided that priority is always given to those who might wish to use it in connection with their employment.

Every user is allocated file space on the computer system so that they may store their own work, whether school work or work in connection with their employment as appropriate, and also any private work within reason. It should be recognised, however, that the school servers are there for educational purposes and large amounts of storage used for personal reasons will not be permitted.

Users will also be given rights to use certain shared resources as well as Internet access and email

All users must respect the privacy of other users. They must **only log on** using the username and password allocated to them. It should be noted that it is not only contrary to school rules to try to log on in any other way, but that it is also a criminal offence under English Law. It is also a criminal offence to try to gain access to computer systems without logging on. It is the user's responsibility to log off the network and check that the logging-out procedure is complete before leaving a computer. If a user suspects that their password has been compromised, they should change it immediately. In any case, passwords will be changed at least once a term. Employees should never, under any circumstances, allow a pupil to use any computer logged on under any employee's logon.

Users must not attempt to connect to the network system any computer that has not been authorised by the ICT Department.

Users must not attempt to access, modify or copy data or passwords that belong to others. They must not attempt to modify any computer in any way; neither must any attempt be made to modify the operation of, or the software on, any machine on the network.

All users must respect copyright. Pupils in particular must not attempt to pass off the work of others as their own whether it is gained from another member of the school or from the Internet. Presenting work of others, particularly in an examination context, will be viewed very seriously and may result in examination entrants being banned, not only from the subject involved, but from all subjects with that examination board.

All users of the system are subject to the Data Protection Act 1998. All users should make themselves familiar with that part of this Act which concerns computers and is set out at the end of these provisions. However, the school cannot be responsible for any data that you process about others and it recommends strongly that you do not do so. If you use data other than for personal use, you should only do so under the terms of the act. The Bursar is the registered officer for the purposes of the Data Protection Act. Exploitation of information, especially for commercial purposes is forbidden.

The computer system is automatically monitored for security violations. If any occur, the system will present a screenshot of the violation for the Computer Systems Manager and management of the school to view. If this suggests that further investigation is required, the school reserves the right to monitor, and on occasion record, actions made by the violator, in order to secure the operation of the system for other users. The school also reserves the right to monitor, and on occasion record, actions where there is strong suspicion of misdeeds. We do this as part of our duty to protect both our pupils and our employees.

In addition, security cameras record activities in the two ICT Centres and the recordings made from them may be consulted to resolve security breaches and any other activity which might endanger the efficient use of the computer system.

In the case of pupils logging on as somebody else, or allowing their password to be known or in the case of other breaches of network discipline, such as leaving computers logged on, or sending email during lessons, the following action will be taken –

- 1<sup>st</sup> Offence: Refer to Director of Pastoral Care, who will record the offence and refer to House Master / Mistress (HsM).
- 2<sup>nd</sup> Offence: Refer to Director of Pastoral Care who will record the offence, and with the HsM impose an appropriate internal punishment. The HsM will inform the pupil's parents.
- 3<sup>rd</sup> Offence: Refer to Director of Pastoral Care who will record the offence, inform the Deputy Head Master and, in consultation with the HsM, will impose a more severe internal sanction. The Director of Pastoral Care will inform parents.
- In any subsequent instances, the matter will be referred by the Director of Pastoral Care to the Deputy Head Master, and suspension from school will be the likely result.

## The Internet

The school has a moral obligation and a legal responsibility to protect pupils from some of the material available on the Internet

The School, ***through its computers and network system only***, provides access to the Internet and email. This is primarily for educational use, but access is also permitted at other advertised times for private use. All users are expected to act responsibly and ensure that any personal use does not breach any of these provisions.

No user should attempt to access pornographic or other undesirable materials from the Internet or any other source including DVDs, CDs and floppy discs, nor should any user take part in any illegal activity. If a user finds pornographic material on his/her computer unexpectedly, either in the form of an e-mail or from a website visited in innocence, the Computer Systems Manager or his assistant should be informed immediately. A pupil or employee who bring pornography into the School, by any means, will incur disciplinary action.

The network element that allows access to the Internet and email systems maintains various logs including the monitoring of sites visited by each individual. The Computer Systems Manager will provide the Deputy Head Master with a copy of the logs of attempted access to blocked sites every two weeks. The Deputy Head Master will review the information and will take appropriate action on the basis of the information received (see Appendix 1).

Where a crime (e.g. deliberately accessing child pornography) has been committed, the school has a duty to inform the relevant authorities.

Downloading files from the Internet is not normally permitted since it poses the risk of importation of viruses, may well break copyright laws and takes up valuable bandwidth slowing the system for other users. Exceptional circumstances may, however, mean that the downloading of a specific file or files is necessary for educational purposes and, for such reasons, application may be made to the Computer Systems Manager for permission.

Every user is allocated an email address. Email is provided for school-related work and for communication with family, friends and colleagues only. Unsuitable language should not be used and may be detected by the monitoring software and reported to the Computer Systems Manager. 'Unsuitable language' includes obscene, inappropriate, threatening, or disrespectful language. Users must not enter chat

rooms or participate in or respond to chain letters. Users must not join any forum or mailing list except for specific educational purposes, in which case application should be made to the Computer Systems Manager for permission. Web-based email will not normally be permitted. We acknowledge, however, that there may be specific difficulties in the case of certain foreign languages, as well as with university and job applications. In these circumstances, users should obtain permission to use the school-approved web mail system from the Computer Systems Manager .

Pupils should not attempt to purchase goods or services or offer goods on any bidding sites through the use of the School Internet system.

Users should remember that inappropriate use of email or the Internet could put their own personal safety at risk. Users should never give personal details, such as names, addresses, telephone numbers, of themselves or other users to others on the Internet. They should certainly never arrange to meet others or enter into financial transactions. Pupils should promptly disclose to a teacher or House Master any message received that makes them feel uncomfortable or that they feel is inappropriate.

Users should always inform the Computer Systems Manager if an inappropriate website is accessed in error, noting the full website address so that future users may avoid accessing it.

The danger of viruses cannot be over-emphasised. Downloading of viruses normally results from a visit to a dubious web-site. They can, therefore usually be avoided by responsible use of the Internet. It is your duty to notify the Computer Systems Manager whenever a virus warning occurs so that it may be dealt with appropriately – remember it might be your work affected or lost if you do not.

In the case of a pupil attempting to access inappropriate material, action will be taken to establish the circumstances and, in particular, whether access was accidental. If it transpires that this is the case, no further action will be taken.

However, in the case of deliberate attempts to access a barred site that contains undesirable material, the following action will be taken:

- in the first instance, referral to the Director of Pastoral Care who will ask HsM to inform parents.
- in the second instance, referral to Director of Pastoral Care who will formally notify parents and impose a sanction, normally a gating in consultation with the HsM.
- in the third instance, referral to the Director of Pastoral Care who will inform the HsM, the Deputy Head Master and parents and a more severe internal sanction, possibly an Old House gating will be imposed.
- in any subsequent instances, the matter will be referred by Director of Pastoral Care to the Deputy Head Master, and suspension from School will be the likely result.
- any further instances will result in permanent ban from Internet and longer suspension.

These offences will be taken into consideration if other instances of misuse of the computer system are apparent (e.g. using another person's access)

### **Data Protection Act**

*Note: The following statement is only applicable to computer-stored information. Separate regulations should be viewed regarding paper-stored information.*

Information can only be kept about persons for specific school-related purposes. The information should be kept to a minimum and for as short a period as necessary. It should be removed when the purpose for its use is completed. Users should not have files of any type on any network servers, local hard disks or on the email system that contain information on a person that they would not like that person to see. Any information that users do keep must be of a factual nature and not hearsay.

Any person may, under the provisions of the act, apply to see information about themselves in order to check the accuracy of the content. To delete such information after an application to view is received is **an offence under the act**.

Users are obliged under the act to take all reasonable steps to minimise unauthorised access to personal information stored on any school computer system. It must therefore be an offence to allow anyone else to use your logon name and password, unless this is specifically for ICT staff to test either your computer or its connection to the network. Never leave any unattended computer logged on for more than a few minutes.

Policy reviewed August 2011 and confirmed as the current Policy

**Dom Leo Maidlow Davis**