ICT ACCEPTABLE USE POLICY

The policies, procedures and information within this document apply to the use of Information and Communications Technology at Reddam House including desktop and laptop computers, tablet devices and cellular phones, and any other device deemed by the Administration to fall under this policy.

Reddam House filters communication and access to websites using Hardware and Software which complies with International Child Protection Standards.

The networks are used for teaching and education and it is therefore deemed that no account on the Reddam House networks is private. This applies to any device which is used by anyone to connect to the Reddam House networks. Any user’s network account may be opened at any time for any reason by a designated network supervisor. Any staff member may check any user's communications at any time. Any device which connects to Reddam House networks may be examined by a designated network supervisor at any time.

Contents

Use of the redam house networks and it facilities

The use the computer facilities at Reddam House, whether it be access on site or remote access via any device, is a privilege granted by Reddam House. Access to the Internet and networks for the purposes of communication and educational research implies that all users agree to abide by the following rules and conditions.

1. Pupils are expected to communicate in a meaningful, respectful and mannerly fashion when using email or any other means of electronic communication. This applies to any email software used in the context of school related communication used on the school premises or externally. Racist or sexist sentiments, hate mail, obscene language, profanity or cyber bullying will not be tolerated. No pupil may initiate or forward any form of Chain email.
2. Any form of communication which brings the name of the school into disrepute will not be tolerated. No person may edit or produce material which denigrates the school, any of its employees or any pupil in the schools. This includes text, graphics, photographs, video or sound files. Pupils must report any occurrence of unacceptable communication to a network supervisor.
3. Pupils are expected to access only those Internet sites which conform to normal legal and moral standards and which are deemed to be acceptable according to the ethos of the school.
4. Pupils should adhere to the rules governing general behaviour throughout the school.
5. Pupils will be held accountable for their behaviour in communicating with any individual or organization which is available through links to the Internet. Pupils must not harass any person or organization by sending unwanted communications.
6. Downloading and uploading of files using school facilities may only be done with permission and under supervision. The misuse of school facilities to download or upload video, sound or game files or protected copyrighted data using a school network computer or wireless connection, will result in the immediate suspension of a pupil's network account.
7. The use of viruses, Trojans or any method of breaking into Reddam House networks will result in immediate permanent banning from the use of Reddam House network facilities.
8. The playing of computer games in school is **completely prohibited at all times**. Subject related educational games may only be used during a timetabled class period under the supervision of the subject teacher. Games related sites may not be accessed. Downloading from games sites is not permitted.

9. No pupils are allowed inside the computer laboratories unless a teacher is present or where specific permission has been granted. There are no exceptions to this rule.
10. Pupils may not use any account other than their own. Pupils are not permitted to divulge their password or share accounts. The current default password should be changed as soon as possible after a user's account has been created.
11. Pupils may only use a device they are working on. Normally, only one person per device will be allowed. Sharing of devices may only occur with permission from the teacher concerned.
12. No transfer media may be brought into the room without permission. Any media which are brought into the room must have been checked for viruses using the currently acceptable virus checking software.
13. Printing may be sent to any of the network printers.
14. No equipment or furniture may be moved from its current position in the Computer Rooms.
15. No eating or drinking is permitted in the Computer Rooms.

Charging of device batteries

1. Devices that are brought to school must be in a fully charged condition. It is the responsibility of pupils to charge their devices each evening.
2. Other than in the case of exceptional circumstances (eg power failure – device left at school overnight etc), pupils will not be able to rely on the ability to charge their device's battery at school.

Screen-savers and desktop backgrounds

1. Inappropriate media may not be used as a screen-saver or background photo.

Sound, music, games or programmes

1. Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
2. Internet games installed on devices at home are not allowed to be played at school, unless permission has been given by the teacher.
3. Pupils are encouraged to have earphones with them should they require sound on the device in use which will be at the discretion of the teacher.

Home internet access

1. Technological device internet access at home is entirely the responsibility of parents and is subject to the structures/rules they have put into place.
2. Parents are encouraged to set appropriate restrictions on internet access and to be vigilant in maintaining these.
3. Reddam House takes no responsibility for any accessibility pupils have to the internet and social media away from its campus, other than to continually instruct, educate and counsel its pupils with regards to cyber safety.

Taking care of technological devices

1. Security and care of an electronic device is both a concern and a priority for both parents and the school.
2. For its part, Reddam House, through its teachers, undertakes to educate its pupils in the correct use and care of technological devices.
3. It is expected that parents will support the education process by reinforcing the best care practice with their children.
4. Pupils are responsible for the general care of their devices while travelling between home and school, and also while at school or involved in any school related activity such as camps or excursions.
5. The responsibility of devices in the home situation is a matter to be determined by parents with their child(ren).

Managing files & saving work

1. Pupils will be taught to save work to a ‘Cloud’ environment using programmes such as Dropbox and Google Drive.
2. It is strongly recommended that parents manage the setup of the Dropbox account as an email address is required for this process. Parents requiring help may seek assistance from the school.
3. Individual teachers will inform parents of their pupils about storage requirements of the work completed, and how best this may be managed.

Software on devices

Software Installed for Non-School Use

1. Pupils, under the supervision of their parents, are permitted to load software/Apps on their devices for use at home.
2. It is assumed that such software/Apps are appropriate in nature; however if deemed unsuitable by the school/teacher, parents will be contacted to discuss the matter.

Parent / guardian responsibilities

Reddam House views the use of technological devices at home as important as their use in the school setting. Parents therefore have an extremely important role in reinforcing and maintaining the practices of safe use of the device, by:-

1. Talking to their child(ren) about values and the standards that they should follow with regard to the use of the internet – just as they do with the use of all media information sources such as television, telephones, movies, radio and iPods.
2. Establishing clear family rules and procedures regarding the use of technological devices at home designed to protect family members from abuse, overuse and addiction to social media.

Insurance

1. It is suggested that parents provide their own insurance via their home and contents policy or by taking out a separate insurance policy for the device to cover its use and possible damage or theft.

School responsibilities

The wireless capacity of technological devices enables pupils to access the internet for information and research and to connect with their peers to communicate and collaborate. With this increased capacity to connect comes an increased need for pupils to understand the ethical and legal (including privacy and copyright) considerations for safe and responsible behaviour online.

To protect pupils from unsuitable content, Reddam House undertakes to:

1. Monitor, and restrict information stored on or transmitted via Reddam House owned equipment and to investigate inappropriate use of resources.
2. Provide staff guidance to aid pupils in doing research and help ensure pupil compliance of the acceptable use policy.

Radicalisation

The Counter-Terrorism and Security Act, 2015, places a duty on Reddam House to prevent people from being drawn into terrorism (“the Prevent duty”). Any form of Radicalisation is therefore forbidden.

Pupil responsibilities

Reddam House places a strong emphasis on pupils managing their devices and taking responsibility for the way in which they are used. Therefore pupils will undertake to:-

1. Use computers/devices in a responsible and ethical manner.
2. Obtain permission prior to recording and/or posting anyone and/or anything on school property or where Reddam House can be identified.
3. Obey general school rules concerning behavior and communication that apply to technological device use.
4. Use all technology resources in an appropriate manner so as to not damage school equipment. This “damage” includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by the pupil’s negligence and/or inappropriate behaviour.
5. Contact a teacher/staff member about any security problems they may have encountered.
6. Monitor their devices and report any suspicious activity.
7. Secure their devices after they have completed working on a task, in order to protect their work and information.