



## **INFORMATION AND COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE POLICY**

REVISED NOVEMBER 2016

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

Reddford 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 Reddford House networks is private. This applies to any device which is used by anyone to connect to the Reddford 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 Reddford House networks may be examined by a designated network supervisor at any time.

### **USE OF THE REDDFORD HOUSE NETWORKS AND IT FACILITIES**

The use of the computer facilities at Reddford House, whether it be access on site or remote access via any device, is a privilege granted by Reddford 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. Students 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 student 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 student in the school. This includes text, graphics, photographs, video or sound files. Students must report any occurrence of unacceptable communication to a network supervisor.
3. Students 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. Students should adhere to the rules governing general behaviour throughout the school.
5. Students will be held accountable for their behaviour in communicating with any individual or organization which is available through links to the Internet. Students 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 student's network account.
7. The use of viruses, Trojans or any method of breaking into Reddford House networks will result in immediate permanent banning from the use of Reddford 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 students are allowed inside the research workroom unless a teacher is present or where specific permission has been granted. There are no exceptions to this rule. This room will be available for students to work quietly, read and study.
10. Students may not use any account other than their own. Students 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. Students 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 only occur with the express permission of a teacher.
14. No equipment or furniture may be moved from its current position in the research workroom.
15. No eating or drinking is permitted in the research workroom.

## **CHARGING OF DEVICE BATTERIES**

1. Devices that are brought to school must be fully charged. It is the responsibility of students to charge their devices each evening.
2. Other than in the case of exceptional circumstances (eg. power failure – device left at school overnight etc.), for logistical reasons students may not be able to charge their device's battery at school.

## **SCREEN-SAVERS AND DESKTOP BACKGROUNDS**

1. Inappropriate or offensive images 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. Students are encouraged to have earphones with them in the event that they require sound on the device in use which will be at the discretion of the teacher.

## **HOME INTERNET ACCESS**

1. 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. Reddford House takes no responsibility for the levels of accessibility students have to the internet and social media away from its campus, other than to continually instruct, educate and counsel its students 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, Reddford House, through its teachers, undertakes to educate its students 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. Students 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. Students 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. Students have access to a controlled Google Drive account via their school Google account.
4. Individual teachers will inform parents of their students about storage requirements of the work completed, and how best this may be managed.

## **SOFTWARE ON DEVICES**

### *Software Installed for Non-School Use*

1. Students, 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**

Reddford 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 etc.
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.

## **SCHOOL RESPONSIBILITIES**

The wireless capacity of technological devices enables students 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 students to understand the ethical and legal (including privacy and copyright) considerations for safe and responsible behaviour online.

To protect students from unsuitable content, Reddford House undertakes to:

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

## **STUDENT RESPONSIBILITIES**

Reddford House places a strong emphasis on students managing their devices and taking responsibility for the way in which they are used. Therefore students 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 Reddford 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 student'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.

## **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.