



Internet Acceptable Use Policy

| | |
|----------------------|---|
| Address | Kinsale Co. Cork |
| Telephone | 0214773174 |
| Email | info@kinsalecommunityschool.ie |
| Website | http://www.kinsalecommunityschool.ie |
| Fax | 0214773184 |
| Date of Commencement | 29 th January 2019 |
| Authors | Ger Hogan/Eddie Farren/John Corocoran |

Kinsale Community School is committed to:

- Enabling all students to fulfil their academic, intellectual, moral, spiritual, social, cultural and physical potential.
- Fostering the development of personal responsibility.
- Engendering a spirit of co-operation and mutual respect among students, staff, management, parents, and the wider community.
- Facilitating the professional development of staff in a safe and caring environment.

Date of ratification by BOM:29/01/2019

Contents

1. Introduction
2. General Approach
3. Desktop Computers
4. Content Filtering
5. Web Browsing and Downloading
6. Email and Messaging
7. Social Media
8. Data Protection
9. Personal Devices
10. Portable Devices
11. Printing
12. Images & Video
13. Cyberbullying
14. School Websites
15. Department of Education issues devices (to students)
16. Permission Form
17. KCS Conduct Guidelines for Microsoft Teams

General Approach

Things to know

The aim of this Internet Acceptable Use Policy (AUP) is to ensure that pupils will benefit from the learning opportunities offered by the school's internet resources in a safe and effective manner.

Internet use and access is considered a school resource and privilege. If the school AUP is not adhered to this privilege may be withdrawn and appropriate sanctions will be imposed.

When using the internet pupils, parents and staff are expected:

- To treat others with respect always.
- Not undertake any actions that may bring the school into disrepute.
- Respect the right to privacy of all other members of the school community.
- Respect copyright and acknowledge creators when using online content and resources.

This Acceptable Use Policy applies to pupils who have access to and are users of the internet in Kinsale Community School.

- It also applies to members of staff, volunteers, parents, carers and others who access the internet in Kinsale Community School.

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Kinsale Community School will deal with incidents that take place outside the school that impact on the wellbeing of pupils or staff under this policy and associated codes of behaviour and anti-bullying policies. In such cases Kinsale Community School will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

Kinsale Community School implements the following strategies on promoting safer use of the internet:

- Pupils will be provided with education in internet safety as part of our implementation of the SPHE and CSPE curriculum.
- Internet safety advice and support opportunities are provided to pupils in Kinsale Community School through our [INDUCTION, PASTORAL CARE, ICT, PEER MENTORING programmes].
- Teachers will be provided with continuing professional development opportunities in internet safety.
- Kinsale Community School participates in Safer Internet Day activities to promote safer more effective use of the internet.

This policy and its implementation will be reviewed annually by the following stakeholders:

- Board of Management

This policy has been developed by a working group including: Principal, Deputy Principal, teachers, pupils, parents/carers, and representatives of the Board of Management.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited).
- Surveys and/or questionnaires of pupils, parents, and teaching staff.

Should serious online safety incidents take place, a member of the school management team should be informed.

The implementation of this Internet Acceptable Use policy will be monitored by all staff, with the support of the ICT co-coordinator and the management team of Kinsale Community School.

Important things to know

- Information Security is everybody's responsibility.
- The School's IT systems are provided for educational use.
- Use of any of the school's IT systems for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this policy.
- The School reserves the right to monitor any aspect of its information systems in order to protect its lawful interests, prevent and/or detect crime, discriminatory and harassing behaviour. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings and may be disclosed to the Gardaí or any other investigatory body.
- This policy refers in several places to things that "Others may find offensive". These include but are not limited to:
 - Pornographic or sexually explicit material
 - Discriminatory and harassing behaviour
 - Tasteless material (such as depiction of injury or animal cruelty)

The School will deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy and associated policies. In such cases the School will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

- The School implements the following strategies on promoting safer use of the internet:
 - Education for students in internet safety as part of the Wellbeing curriculum.
 - The School participates in Safer Internet Day activities
 - Teachers will be provided with CPD opportunities in the area of internet safety.
- Should serious online safety incidents take place, the Designated Liaison Person (DLP) for child protection, the Principal-Mr Fergal McCarthy, should be informed.

Things to do

- ✓ Always treat others with respect.
- ✓ Respect the right to privacy of all members of the school community.
- ✓ Respect copyright and acknowledge creators when using online content and resources.
- ✓ Exercise care and common sense in your use of information technology.
- ✓ Refer to the glossary at the back if you need a definition of any term in this document.

Things not to do

- ✗ Anything illegal.
- ✗ Anything that contravenes this policy
- ✗ Anything that will harm the reputation of the School.
- ✗ Anything that contravenes Code of Behaviour and Anti- bullying Policy

Desktop Computers

Things to know

- Desktop computers are the property of the School and have been prepared by the IT department for use on the School network.
- Authorised software is installed on your computer and you are not allowed to install anything on your own.
- Data saved to local (usually C: and D:) drives will not be backed up, and will be lost if the computer breaks, gets stolen or is replaced. Therefore, it is highly recommended, and it is your responsibility to store all your data on your personal One Drive account.
- The School may at any time and without prior notice:
 - Audit the computers to ensure compliance with policy.

Things to do

- ✓ Log off from any workstation (CTRL+ALT+DEL) once you are finished using it.
- ✓ Save data to your personal One Drive (Office 365 account).
- ✓ Ensure that files received from anywhere outside the School are virus checked before you open them. This includes files on CD or USB drive. If in doubt, ask the IT Co-ordinator to scan it for you.
- ✓ If you suspect a computer you are using may have a virus, leave the computer on, unplug the network cable and call the IT Co-ordinator.
- ✓ Turn any PC and monitor off at night to save energy unless there is a specific reason to leave it on.

Things not to do

- ✗ Do not allow anyone else to use a computer while you are logged in.
- ✗ Never install software on your computer. This should only be done by the IT Co-ordinator or the ICT Team.
- ✗ Things that you should never attempt to install include but are not limited to:
 - ✗ Screen savers and games, music download software
 - ✗ Utilities that claim to remove spyware or viruses
 - ✗ News readers or ticker-tape services
 - ✗ Applications that download torrents such as showbox, popcorn, moviebox etc
 - ✗ Do not disable or uninstall any of the software that is installed on your computer

Content Filtering

Things to Know

Kinsale Community School has chosen to implement the following level on content filtering on the Schools Broadband Network (Education18)-only school devices can be used on this network.

Level 4 This level allows access to millions of websites including games and YouTube but blocks access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

A second WIFI network (ASDWIFI) located in the G corridor does not have a PDST filter (as above). This network is for staff personal devices. Under no circumstances are students permitted to have access to this network.

Pupils taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Web Browsing and Downloading

Things to Know

Pupils will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

Pupils will report accidental accessing of inappropriate materials in the classroom to their teacher.

Pupils will report accidental accessing of inappropriate materials in school but outside the classroom to the relevant Class Teacher or Year head

Pupils and staff will not copy information from the internet without acknowledging the creator and referencing the source of the content.

Pupils and staff will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Pupils will use the school's internet connection only for educational and career development activities.

Pupils will not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.

Pupils will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Use of file sharing and torrent sites is not allowed
- Downloading by pupils of materials or images not relevant to their studies is not allowed.

Things to do

- ✓ Use the school's internet connection for educational and career development activities only.
- ✓ Report accidental accessing of inappropriate materials to the teacher or IT Co-ordinator.
- ✓ Sites that are blocked usually ask you to click on a particular section to fill in a request to have the site reviewed by the NCTE as appropriate for teaching purposes. Please use this method of getting sites unblocked as the IT Co-ordinator has no control over unblocking sites.
- ✓ If you suspect a computer you are using may have a virus or spy-ware infection, leave the computer on, unplug the network cable and call the IT Co-ordinator.

Things not to do

- ✗ Do not view or download anything that others may find offensive, illegal, obscene and defamatory. This includes, but is not limited to:-
- ✗ Pornography, Racism, Terrorist sites
- ✗ Do not upload or download large files that results in heavy network traffic and affect performance for other users.
- ✗ Do not download anything that is likely to be covered by copyright. This includes, but is not limited to:-
 - ✗ Music, Pictures, Software and Movies
 - ✗ Do not visit the "high-risk" site categories shown below. Although their content appears to be free,
 - ✗ it is often funded by installing spyware on your computer.
 - ✗ Free screensavers and smileys
 - ✗ Free music downloads or ring tones
 - ✗ Free software and serial numbers (also known as cracks)
 - ✗ Adult material
 - ✗ Films from streaming sites (moviebox)
- ✗ Do not download any attachments using personal web-based mailboxes (Yahoo, Hotmail etc.) as it is not monitored by the School security software.
- ✗ Do not listen to the radio stations through internet as the radio stream consumes too many resources in the network that will affect performance.

Email and Messaging

Things to know

Pupils will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Pupils will not use school email accounts for personal emails.

Pupils should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils should avoid opening emails that appear suspicious. If in doubt, pupils should ask their teacher before opening emails from unknown senders.

- The School's e-mail systems are provided for school use. Reasonable personal use is permitted provided it is lawful, ethical and takes place during authorised breaks.
- The School reserves the right to monitor all e-mail to ensure compliance with policy
- E-mail is not a secure method of communication. Once a message is sent you have no further control over who reads it.
- E-mail is admissible evidence in any legal proceedings and carries the same weight as a letter on school headed paper.
- School email accounts may not be used to register for online services such as social networking services, games and purchasing.
- Students will use approved email accounts only under supervision by or permission from a teacher.
- The use of personal email accounts is only allowed at Kinsale Community School with expressed permission from members of the teaching staff.
- Pupils should not under any circumstances share their email account login details with other pupils.
- Pupils should not use school email accounts to register for online services such as social networking services, apps, and games.
- Pupils will use approved class email accounts only under supervision by or permission from a teacher.
- Pupils should be aware that email communications are monitored.

Things to do

- ✓ Use the same care when drafting an e-mail message as you would when writing a letter or memo on school headed paper.
- ✓ Make sure that your message is concise, relevant and sent only to the people that need to read it.
- ✓ Check your e-mails every day and clear out old and unwanted messages from your mailbox.
- ✓ Return any wrongly delivered message to the sender. If it contains confidential information, it should not be disclosed or used in any way.
- ✓ Immediately report to the Principal the receipt of any communication that makes you feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and do not respond to any such communication.

Things not to do

- ✗ Never open an attachment that you were not expecting, even if you know the sender.
- ✗ Do not use personal emails accounts for any school communication or business.
- ✗ Do not use e-mail to send sensitive or confidential information.
- ✗ Do not send or forward anything that:
 - ✗ Is illegal, obscene, others may find offensive, may be defamatory or harassing
 - ✗ Is covered by a copyright (pictures, movies, music, others)
- ✗ Do not circulate non-school-related material. This includes but is not limited to:-
 - ✗ Chain letters, jokes, virus warnings, software
- ✗ Never use e-mail to rebuke, criticise or complain about somebody. You may say something that you regret, and the record will be permanent.
- ✗ Never supply banking or payment details in response to an e-mail message. This is a well-known method of fraud. Your bank will never request security details by e-mail.

Social Media

Things to Know

The following statements apply to the use of messaging, blogging and video streaming services in Kinsale Community School:

- Use of instant messaging services and apps including Snapchat, What's Apps, G Chat etc. is not allowed in Kinsale Community School.
- Use of blogs such as Word Press, Tumblr etc. is allowed in Kinsale Community School with express permission from teaching staff.
- Use of video streaming sites such as YouTube and Vimeo etc. is with express permission from teaching staff.

Staff and pupils must not use social media and the internet in any way to harass, insult, abuse or defame pupils, their family members, staff, other members of the Kinsale Community School community

Staff and pupils must not discuss personal information about pupils, staff and other members of the Kinsale Community School community on social media.

Staff and pupils must not use school email addresses for setting up personal social media accounts or to communicate through such media.

Staff and pupils must not engage in activities involving social media which might bring Kinsale Community School into disrepute.

Staff and pupils must not represent your personal views as those of Kinsale Community School on any social medium.

Things to do

- ✓ Use the twitter account and Blogs in a safe and respectful manner.
- ✓ Use blogs for educational purposes.
- ✓ Use Twitter as a means of communicating activities and achievements of KCS students.
- ✓ Always treat others with respect.
- ✓ Report any incident of cyber bullying to the relevant Class Teacher/Yearhead/Deputy Principal/Principal.

Things not to do

- ✗ Do not use social media in any way to harass, insult, abuse or defame students, their family members, staff, other members of the school community.
- ✗ Do not discuss personal information about students, staff and other members of the school community on social media.
- ✗ Do not represent your personal views as those of being Kinsale Community School on any social medium.

Data Protection Responsibilities

Things to know

- You are personally responsible for ensuring the confidentiality of a student's personal data.
- Student information is now accessible on Office 365 and CloudSchool which is password protected.
- If student information is put onto a USB, the files on the USB must be encrypted.

Things to do

- ✓ Log off from any workstation (CTRL+ALT+DEL) once you are finished using it.
- ✓ When distributing information use codes/abbreviation rather than names.
- ✓ If Personal Data is saved to a USB drive ensure it is fully encrypted.
- ✓ If you process personal data (data that identifies a living individual) during your work, you must do this in accordance with General Data Protection Regulation (GDPR) May 2018.

Things not to do

- ✗ Do not view sensitive information on the train, plane or in any public area. This provides an opportunity for onlookers.
- ✗ Do not allow family, friends or anybody else to use the computer which contain student information.
- ✗ When communicating information through email do not put names in the subject bar.
- ✗ Do not disclose or share any sensitive information to other people if not under the expressed authorisation of the Principal.
- ✗ Do not leave printed documents around the printer as they may contain confidential data.

Personal Devices

Pupils using their own technology in school should follow the rules set out in this agreement, in the same way as if they were using school equipment.

The following statements apply to the use of internet-enabled devices such as tablets, gaming devices, and digital music players in Kinsale Community School

- Pupils are only allowed to bring personal internet-enabled devices into Kinsale Community School with expressed permission from staff.
- Pupils are only allowed to use personal internet-enabled devices during lessons with expressed permission from teaching staff.
- Pupils are only allowed to use personal internet-enabled devices during social time with expressed permission from staff.

Portable Computers

Things to know

- Portable computers are the property of the School and have been prepared by the IT department for use on the School network.
- Authorised software is installed on the Portable computers and you are not allowed to install anything on your own.
- Data saved to local (usually C: and D:) drives will not be backed up, and will be lost if the tablet breaks, gets stolen or is replaced, therefore it is highly recommended, and it is your responsibility to store all your data on your personal One Drive account.
- You are responsible for the care and safe storage of any computer equipment that has been issued to you and are taking full responsibility for everything done on that portable computer.
- The term 'portable computer' covers any school-owned mobile computing device including:-
 - Laptop or tablet PCs (ipads)

Things to do

- ✓ Save work to One Drive rather than the portable computer.
- ✓ Ensure that files received from anywhere outside the school are virus checked before you open them. This includes files on CD or USB drive. If in doubt, ask the IT Co-ordinator to scan it for you.
- ✓ Always consider the physical security of your portable computer:-

| | |
|------------------------------|---|
| In an unlocked office | Kept in a locked drawer |
| In the car | Do not leave your portable device in the car. While in transit it must be stored in the boot of the car. |
| At home | Ideally within a locked work area. Otherwise within a locked drawer |
| In a hotel | Suitcase or safe. |
| Travelling | Concealed from view. Always keep the computer on your person and out of sight and locked away. |

Things not to do

- ✗ Do not allow family, friends or anybody else to use the computer.
- ✗ Do not use devices for personal purposes
- ✗ Do not download any software or apps that are not preapproved by the IT Co-ordinator.
- ✗ Do not use apps that use torrents to download or stream music or movies.

KCS Guidelines for Staff on Portable Computers and Surface devices 20/21

Things to know

- Any issues or questions in relation to portable devices or surfaces should be directed toward ICTSupport@kinsalecommunityschool.ie.
- Portable computers are the property of the School and have been prepared by the IT department for use on the School network.
- Authorised software is installed on the Portable computers- do not install anything yourself without consulting the IT Dept.
- You can download apps from the Microsoft store. If you need an app not available in the Microsoft store, please contact the IT Dept.
- Data saved to local (usually C: and D:) drives will not be backed up, data will be lost if the tablet breaks, is stolen or replaced, therefore it is your responsibility to store all your data on your OneDrive account.
- You are responsible for the care and safe storage of any computer equipment that has been issued to you- any damage to the portable computer is your responsibility and in the event of a loss, it must be replaced by you. You may insure it if you wish.
- A review of portable computers at KCS will take place after five years.
- The term 'portable computer' covers any school-owned mobile computing device including Laptop or surface devices.

Things to do

- ✓ Save work to One Drive rather than the portable computer.
- ✓ Ensure that files received from anywhere outside the school are viruschecked before you open them. This includes files on CD or USB drive. If in doubt, ask the IT Co-ordinator to scan it for you.
- ✓ Always consider the physical security of your portable computer:

| | |
|------------------------------|---|
| In an unlocked office | Kept in a locked drawer |
| In the car | Do not leave your portable device in the car. While in transit it must be stored in the boot of the car. |
| At home | Ideally within a locked work area. Otherwise within a locked drawer |
| In a hotel | Suitcase or safe. |
| Travelling | Concealed from view. Ideally locked in a Keep the computer on your person and out of sight at all times |

Things not to do

- ✗ Do not allow family, friends or anybody else to use the computer.
- ✗ Do not use devices for personal purposes.
- ✗ Do not download any software or apps that are not preapproved by the IT Dept.
- ✗ Do not use apps that use torrents to download or stream music or movies.

Printing

Things to know

- Colour printers cost are at least 10 times more expensive per page than black and white ones, even if there is no colour on the page.
- Printers are provided for education use only.

Things to do

- ✓ Be selective about what you print. Print only when necessary and only the necessary pages of a document.
- ✓ Double sided printing as set as a default setting on all the printers to save paper.
- ✓ Use a photocopier when producing many copies.
- ✓ Keep the area around printers tidy.

Things not to do

- ✗ Do not print to a colour printer unless colour conveys important information in your document that would be lost in black and white.
- ✗ Do not resend your print job if nothing happens. Instead, check the following:-
 - ✗ Is the print job still listed in the queue?
 - ✗ Is the printer switched on?
 - ✗ Is the printer in an error state because:-
 - ✗ It is out of paper
 - ✗ It is out of toner or ink
 - ✗ If any of those occurs please contact Reception or the IT Coordinator.
- ✗ Mindless printing is an offence to carbon footprint
- ✗ Do not leave printed documents around the printer as they may contain confidential data.

Images & Video

Things to know

Care should be taken when taking photographic or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

At Kinsale Community School pupils must not take, use, share, publish or distribute images of others without their permission.

Taking photos or videos on school grounds or when participating in school activities is allowed once care is taken that no harm is done to staff or pupils of Kinsale Community School.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Pupils must not share images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside.

Sharing explicit images and in particular explicit images of pupils and/or minors is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other pupils automatically incurs suspension as a sanction.

Cyberbullying

Things to know

When using the internet pupils, parents and staff are always expected to treat others with respect.

Engaging in online activities with the intention to harm, harass, or embarrass another pupil or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.

Measures are taken to ensure that staff and pupils are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyber-bullying even when it happens outside the school or at night.

Measures are taken by Kinsale Community School to ensure that staff and pupils are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyber-bullying even when it happens outside the school or at night.

Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and will be dealt with, as appropriate, in accordance with the school's code of behaviour.

The prevention of cyber bullying is an integral part of the anti-bullying policy of our school.

School Websites

Pupils will be given the opportunity to publish projects, artwork or school work on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.

The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.

Webpages allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content.

The publication of student work will be coordinated by a teacher.

Kinsale Community School will use only digital photographs, audio or video clips of focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission.

Personal student information including home address and contact details will not be published on Kinsale Community School web pages.

Kinsale Community School will avoid publishing the first name and last name of pupils in video or photograph captions published online.

Department of Education issued devices (for Students)

Please refer to circular number 0010/2013 for full details on allocation, responsibilities and maintenance of these devices.

Acceptable Use Policy-Permission Form

Legislation: The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with: Data Protection (Amendment) Act 2003, Child Trafficking and Pornography Act 1998, Interception Act 1993 Video Recordings Act 1989, The General Data Protection Regulation-GDPR (2018).

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

Parent Signature: _____ Date: _____

Address:

Please review the school Internet Acceptable Use Policy on the school website at <https://www.kinsalecommunityschool.ie/policies>, and sign and return this permission form to the school office.

I agree to follow the school's Acceptable Use Policy on the use of the Internet. I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Student's Signature: _____ Year Group: _____

Parent/Guardian: _____

Date: _____

KCS Conduct Guidelines for Teams

Ratified by BOM 22/01/2021

1. Students should follow teacher directions in relation to camera use. In general, participants should begin every Teams meeting with the camera turned off, and should only turn their camera on after the teacher has indicated that it is appropriate to do so.
2. Participants should begin Teams meetings with their microphones muted and only unmute them when they are speaking. It is polite to keep microphones muted when not speaking in order to minimise feedback and disruption for those who are speaking. Students are responsible for anything that can be heard through their microphone. We understand, at the same time, homes can be busy.
3. Students may not send private messages to other participants during a Teams meeting unless explicitly instructed to do so by the teacher as part of a learning activity.
4. Under no circumstance may any aspect of the Teams meeting be recorded/photographed in any way by anyone except the teacher. This includes recording directly using the Teams record function, using an outside piece of technology, like a phone or an iPad or taking screenshots or screen recordings of a meeting. Students should be aware that Teams meetings may be recorded by the teacher and teachers will alert them to this. Students are responsible for the activities associated with their Office 365 account during Teams meetings
5. Parents/ guardians should be aware that students will be participating in Teams meetings at various times throughout the school week. A parent/guardian is welcome to contact the teacher to discuss the Teams meeting if they have any concerns. Teachers will respond during working hours.
6. Students must ensure that they are appropriately dressed (ie. a PE half-zip or other similar neat and tidy clothing is suggested) and in a suitable environment for the duration of the Teams meeting. It is the student's responsibility to ensure that they are dressed appropriately and that there is nothing inappropriate and/or offensive in the environment from which they are communicating. It is recommended that students use a plain or school-related background setting for privacy.
7. During Teams meetings, students are expected to be respectful and courteous at all times to all participants. Students should not do or say anything with the intention of hurting or offending other participants. No student should make personal remarks about other participants.
8. If a student feels uncomfortable about the conversation in a Breakout Room, they should leave it and notify the teacher. Students should be aware that the teacher will 'visit' the Breakout Room to monitor the session (they can hear and see what is going on, including chats).
9. Students should only use a photograph of themselves on their Teams/365 and not use photographs of any other individuals, celebrities, pets or images that may be inappropriate in any way. The purpose of the photo is to identify the student so if the student is not

comfortable with a picture of themselves, they should leave empty so that the teacher can see their initials.

If the teacher feels that any of the above guidelines have been breached, they may remove a student from the meeting without notice. The school's code of behaviour, acceptable usage policy, disciplinary procedures and any other relevant policy will be applicable for the duration of any Teams meeting or online learning activity.