

Scoil Bhríde Clane, Co Kildare
Roll No.: 19797E, RCN No.: 20124960
Principal: Mrs. Eimear Hennessy

Acceptable Usage Policy (AUP)

Introduction

The Internet is a valuable teaching and learning tool. It provides information and allows people to communicate with others and share information. It can develop children's independent research skills and promote life-long learning. However, in its largely unregulated state, the internet can also present a number of risks for children and therefore these guidelines will be followed when using the internet in school. This policy should be read in conjunction with the school's Code of Behaviour, Anti-bullying Policy, Child Safeguarding Statement, Health and Safety policy, Data Protection Policy, Mobile Phone Policy. The Acceptable Use Policy applies to pupils, staff members, volunteers, carers and others who have access to and are users of the internet in Scoil Bhríde. The Acceptable Use Policy applies to all of the school's devices including all computers, iPads, laptops, smartphones and other IT resources that connect to the school's network.

Aims

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

Pupils Use of the Internet

Internet use and access is considered a school resource and privilege. If the AUP is not adhered to, this privilege may be withdrawn and appropriate sanctions will be imposed. Pupils are responsible for their own good behaviour on the internet. Access to the internet may be withdrawn from pupils who fail to maintain acceptable standards of use. Internet access in the school includes a filtering service to minimise the risk of exposure to inappropriate material. However, no filtering service is completely fool-proof and therefore pupils will be supervised during the use of the internet. Staff will ensure to the maximum extent possible, that pupils know and understand that no internet user is permitted to:

- Use the internet for any illegal activity including accessing other computers.
- Retrieve, send, copy, or display offensive messages or pictures.
- Use obscene or offensive language.

➢ Cause damage to computers, computer systems or networks.
➢ Violate copyright laws.
➢ Disclose or publicise their own or another person's personal information.
➢ Use another user's password.
➢ Trespass in another user's folders, work or files.
➢ Cause any form of vandalism to the machine or the work of others including the uploading or creation of viruses.
Parents consent to their child using the internet in school and agree to abide by the school policy.

Organisation and Management of Internet Use
Teachers will select sites which will support pupils' learning. Pupils may be given details of suitable sites to extend their learning at home as and when appropriate.
Access to age appropriate and education apps are on school devices.
Only members of the Digital Learning Team are sanctioned to download school-based apps.

Promoting Safe and Independent Use of the Internet
Internet access in school will be supervised. Teachers will ensure that pupils understand appropriate use of the internet and are aware of the rules. Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Children's Use of Email, Messaging and Social Networks
In the event of remote learning being implemented, pupils in senior classes will be provided with an email address as part of the allocation of Microsoft 0365. These email addresses will be used to sign in to Microsoft and other apps used in conjunction with Office 365 e.g. Microsoft Teams.

The use of chat rooms, messaging services or social networking sites is forbidden unless for school use and teacher permission is given.

Social Media
- The following statements apply to the use of messaging, blogging and video streaming services in Scoil Bhríde.
- Use of instant messaging services and apps including Snapchat, Whats Apps is not allowed in Scoil Bhríde.
- Use of blogs such as Word Press, Tumblr etc. is prohibited.
- Use of video streaming sites such as YouTube and Vimeo etc. is allowed under staff supervision at certain times in Scoil Bhríde.
- 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 Scoil Bhríde community
- Staff and pupils must not discuss personal information about pupils, staff and other members of the Scoil Bhríde 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 Scoil Bhríde into disrepute.
- Staff and pupils must not represent your personal views as those of bring Scoil Bhríde on any social medium.

Staff Use of Email and the Internet
Members of staff are encouraged to use various online resources in their teaching and learning activities, to conduct research and for contact with others. Each member of staff has access to a school email address as part of his/her work, protected by the use of a confidential password which should be kept secure.

- When using the internet, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws.
- School printers may be used to print downloaded materials associated with school activities.
- All users are expected to communicate in a professional manner.
- It will not be usual practice to read staff emails but the school reserves the right to do this in the case of a suspected breach of these policy guidelines.
- A serious breach may be treated as a disciplinary matter.
- No person will in any way alter the filtering preferences.

School Strategies
The school employs a number of strategies in order to maximise learning opportunities and reduce the risks associated with the Internet. These strategies are as follows:

General
- Internet sessions will always be supervised by a teacher
- Filtering software and/or equivalent systems will be used to minimise the risk of exposure to inappropriate material. The school currently uses the OIDE content filtering level four.
- Websites will be previewed and evaluated by a teacher before being integrated into lessons conducted using school devices.
- Staff will supervise pupils' Internet usage.
- The leadership team may review browsing history on school devices.
- Pupils will participate in Safer Internet Day. Webwise resources will be used to support and heighten awareness of internet safety.
- Teachers are advised to upskill using the Webwise website.
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis
- The use of external drives, memory sticks, CD-ROMS, or other digital storage media in school requires a teacher's permission.
- Pupils will treat others with respect at all times and will not undertake any actions that may bring themselves, their family or the school into disrepute.

Internet
- Internet will be used for educational purposes only
- Pupils will seek permission before entering any Internet site, unless previously approved by a teacher
- 'YouTube' (and similar sites) can be accessed only under the supervision and direction of the teacher.
- 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 accordance with school procedures.
- Pupils will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement)
- Pupils will never disclose or publicise personal information
- Downloading materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.
- Pupils 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 are not permitted to use internet chat rooms.

Email:

Pupils

- If deemed appropriate, pupils in senior classes may be assigned a school Microsoft office 365 account for sending or receiving emails with the permission of class teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Pupils will not reveal their own or other people's personal details, such as addresses, telephone numbers, email addresses or pictures.
- Pupils will never arrange face to face meeting with someone they only know through emails or the internet.

Contact with staff members

- Pupils will never use personal email accounts to contact the teacher.
- Aladdin Connect: The school uses the Aladdin Schools software service www.aladdin.ie for administrative purposes. The Aladdin Connect portal is part of this and gives secure access to messages from the school and to details of a child's attendance, test results, support documents, reports cards etc. Teachers can use the noticeboard to communicate with parents.

Cyber-bullying

When using the internet pupils, parents and staff are expected to treat others with respect at all times.
The prevention of cyber bullying is an integral part of the anti-bullying policy of our school.
Measures are taken by Scoil Bhride to address cyber bullying are outlined in our Bí Cineálta/KIVA policy.
Engaging in online activities with the intention to harm, harass, or embarrass another pupil or member of staff is an unacceptable and absolutely prohibited behavior.

Artificial Intelligence

- Scoil Bhride recognises the potential benefits of Artificial Intelligence (AI) in education and is committed to its responsible and ethical use within our learning environment.
- Scoil Bhride provides opportunities for training and professional development for teachers to effectively utilise AI tools in their teaching practices, ensuring they stay up to date with technological advancements.
- The selection of AI tools and technologies in Scoil Bhride aligns with educational goals, including supporting learner agency and promoting critical thinking.
- AI technologies are integrated into the curriculum to enhance learner outcomes and experiences.
- Scoil Bhride integrates AI into its educational processes to enhance learning, foster innovation, and promote the development of critical skills.
- A regular review of the impact of AI on learning outcomes is to be conducted to ensure continuous improvement.
- All AI tools authorised for use in Scoil Bhride comply with data protection regulations (GDPR).
- Entering personal, sensitive, or confidential data into any AI system without proper authorisation is strictly prohibited.
- Learners will not create, share or send any AI generated material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Staff and learners must not use AI in any way to harass, insult, abuse or defame learners, their family members, staff, other members of the Scoil Bhride community
- Staff and learners must not engage in activities involving AI generated material which might bring Scoil Bhride into disrepute.

- Scoil Bhride promotes digital literacy and critical thinking skills to help learners understand AI, its implications, and responsible usage. This includes data literacy, verification of AI-generated information, and recognising potential biases in AI tools.
- AI systems used in Scoil Bhride ensure fairness, transparency, and accountability in decision-making processes.
- Learners must attribute AI text and images properly when used in assignments/homework.
- Teachers will attribute AI text and images when used.
- AI Generated material is allowed for the purpose of research, brainstorming, revising text.
- AI Generated material may be allowed for certain activities with prior school permission.
- If used for research learners must factcheck, check other sources and reference sources.

- AI systems must not be used to infer or assess the emotions of pupils, staff or other persons within the school, except where the use falls within a legally permitted medical or safety exception and has been specifically approved by the school.

- AI systems must not be used within the school for any of the following purposes:
- determining access or admission to the school, or assigning pupils within the education system;
- evaluating or scoring pupils' learning outcomes where the AI system itself performs or materially determines the assessment;
- determining the appropriate level of education, educational pathway or educational support that a pupil should receive or be able to access; or
- monitoring or detecting prohibited behaviour by pupils during tests or examinations.

- Personal, confidential or sensitive information must never be entered into a free or consumer-grade AI service. Pupil information, health information, safeguarding information, behavioural or disciplinary information, assessment information and any other confidential school information is within this prohibition.
- Staff and pupils should only use AI in a school context where they have received appropriate guidance or training on its use. For pupils, use should also be age-appropriate and, where appropriate, form part of a teacher-directed or supervised activity. (training to be provided to staff during the 2026/2027 school year.

Distance Learning

In circumstances where teaching cannot be conducted on the school premises, teachers may use the school website, Microsoft Office 365, Seesaw, or other platforms approved by the Principal and the Board of Management to assist with remote teaching where necessary. The school has signed up to the terms of service of the Online Platforms in use by the school. The School has enabled the most up to date security and privacy features which these Online Platforms provide. Staff are encouraged to engage with CPD for the platforms used. See Appendix on Distance Learning Safety Guidelines for Staff.

The following rules must be complied with through the use of Zoom and Microsoft Teams:

- For the purpose of the video call, the pupil must engage from a suitable location within their home.
- The video camera must be kept on for all calls.
- A parent or guardian must be in close proximity at all times during the call.
- No recording, uploading or sharing of the call in any format is permitted.
- This is a virtual classroom setting and should be treated with the same level of respect as they would if they were in school.

See Appendix B for Virtual Meeting Etiquette

The school will provide resources and/or advice to parents/pupils relating to internet safety. See appendix C for Advice for parents on ICT in the Home.

When students engage in "remote teaching and learning" through the school Office 365 platform i.e Microsoft Teams, Seesaw or Zoom, normal school policies apply regarding behaviour, ICT usage, Bí Cineálta etc
The teacher will initiate and invite the students to the meeting.
It will be at the discretion of the class teacher as to whether the microphone functions are turned on or off.
Cameras must be turned on.
Meetings may be recorded by the teacher to share with any students who were unable to attend. The teacher will inform the class at the start of the meeting if they will be recording the meeting for this purpose.
Students are not permitted to record or take photographs of meetings.
When the teacher informs the class that the meeting is over, all students must press the 'leave' button.
The teacher is the last person to leave the meeting.

SNA's may use Microsoft Teams, Zoom or phone calls to connect with their students during times of remote teaching and learning.

Photos and Videos
Photographs and digital images including videos of school events are taken from time to time in our school. These photographs and videos may be published around the school, on our website, through Seesaw or Microsoft Teams, in newsletters, calendars and local and national newspapers. In the case of the website, pupils' names will not be recorded with the picture. Permission for these photographs and videos is sought from parents/guardians through Aladdin Connect. Staff will ensure to review permission for pupils in their class prior to sharing photos or videos. Parents/guardians must not share these digital images through social media, especially images featuring other pupils with their daughter.

School Website
Designated teachers and Parents' Association Members will manage the publication of material on the school website.

- Personal pupil information, home addresses and contact details will not be published on the school website
- Class lists will not be published
- Pupils' full names will not be published beside their photograph
- Digital photographs, video clips and audio clips will focus on groups and group activities rather than on individual pupils
- Pupils will be given an opportunity to publish projects, artwork or school work on the school website on the school newsletter.
- Staff will seek permission to publish a student's work will be sought from pupils/ parents/ guardians. This permission may be withdrawn at any time.
- Pupils will continue to own the copyright on any work published

Education
21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time, they need to learn to recognise and avoid these risks – to become internet wise.
Resources that may be used to implement this programme include
Use of sections pertaining to children, parents and staff on www.webwise.ie website

Filtering

'Filtering' is a term used to describe a way of limiting the content of web pages, emails, chat rooms and other electronic data to which users may be exposed. No filter is 100% accurate. The most effective filtering tool is adult vigilance.

Many browsers have their own built in filtering tool e.g. Google. Google's search engine has a built-in "Safe Search". This filter eliminates sites that contain pornography and explicit sexual content from search results. It is easily applied by clicking on the Preferences link on any Google page. Unfortunately, it is also easily removed.

Scoil Bhríde has filtering software. The access to websites from all school computers is monitored and regularly reviewed by the NCCA. Websites are only allowed through following a verification of their suitability. Our school uses filter level 4 (see Appendix E)

Firewalls
Windows XP has a built-in firewall. Firewall software can be purchased or downloaded free from the Internet. Scoil Bhríde has installed firewall software through our IT support company GDK.

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

Communication Technology	**Allowed**	**Allowed in certain times**	**Allowed with teacher permission**	**Not allowed**
Mobile phones may be brought to school.	√			
Use of mobile phones in lessons.			√	
Use of mobile phones in social times.			√	
Taking photos on mobile phones or other camera devices			√	
Use of smart watches, handheld devices e.g., tablets, Nintendo, kindles DS.		√		
Use of personal email address in school.			√	
Use of school email address for personal use.				√
Use of chat rooms/ facilities.				√
Use of instant messaging.				√
Use of social media sites.				√
Use of blogs				√

Communication
A copy of this policy is available for staff and parents to view in the school and on the school website.

Ratification
This policy was ratified by the Board of Management on the 11th January 2021. It was reviewed following the period of remote teaching and learning on 15th March 2021.

This policy was reviewed by the Leadership and Management Team in May 2024.
This policy was reviewed by the Leadership and Management Team in September 2026

Signed: Eimear Hennessy Date: 20.10.26
(Principal)

Signed: Peter Cook Date: 20-10-26
(Chairperson, Board of Management)

Appendix A:

Distance Learning Safety Guidelines for Staff

Staying safe
It is important that teachers maintain the safe and ethical use of the internet during distance learning and assist parents and guardians to be aware of their role also. There are helpful resources available at https://www.webwise.ie/ to support teachers, parents and students.

Zoom
The following precautionary measures should be taken when using Zoom with your class.

- Review your account settings prior to organising your meetings.
- Check the permissions section on Aladdin Connect to ensure your pupils have permission to use Zoom prior to sending a link.
- Ensure that the "Waiting Room" function is activated in your account settings.
- Ensure that only names known to you, the name of the child in the class is admitted to the meeting from the lobby.
- Ensure that a password is needed for participants to join the meeting.
- Once all participants have joined your meeting, lock the meeting.
- Participants should not be able change their video background.
- Ensure that participants cannot change their name.
- Once the meeting has ended, the host/teacher must be the last to leave the meeting.
- Familiarise yourself with the process of removing a participant from a meeting should the need arise.
- Exercise care if enabling the "share screen" function for participants.

Consult the sites below for further information:

- Best practices for securing your virtual classroom:https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-you r-virtual-classroom/
- Tips on security: https://zoom.us/docs/en-us/privacy-and-security.html

Seesaw:
The following precautionary measures should be taken when using Seesaw with your class:

- Check the permissions section on Aladdin Connect to ensure your pupils have permission to use Seesaw prior to sending access codes.
- Review your account and class settings prior to using the platform with your class.
- Check your "display name" in your account settings to ensure your privacy is protected.
- When sharing access codes with your pupils' parents/guardians, do so securely through the use of email, text or Aladdin Connect.
- Be sure to sign out of your account every time you have finished using your account.
- Encourage pupils and parents to sign out of their accounts when they have finished using their account.

Review class settings to ensure that:

- Student comments are disabled.
- Students are unable to see each other's work.
- "New items require approval" setting is enabled.

- Class Blog should be disabled.

Microsoft Office 365:
The following precautionary measures should be taken when using Microsoft Office 365 with your class:

- Check the permissions section on Aladdin Connect to ensure your pupils have permission to have a Microsoft Office 365 account prior to assigning account information.
- Pupils must be made aware of the importance of not sharing their log in details with others.

Microsoft Teams:
The following precautionary measures should be taken when using Microsoft Teams with your class:

- The teacher sets up a scheduled time for a call.
- Set up a lobby to admit children to the meeting.
- Once the meeting has ended, the teacher must be the last to leave the meeting.
- Familiarise yourself with the process of removing a participant from a meeting should the need arise.
- Exercise care if enabling the "share screen" function for participants.

Zoom Privacy Policy: https://zoom.us/privacy
Seesaw: https://web.seesaw.me/privacy-policy
Microsoft Teams: https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide

Appendix B:

Virtual Meeting Etiquette (Zoom or Microsoft Teams)

1. Scoil Bhríde may use online meetings if we are closed for extended periods. To help us get the most benefit from these, we ask that the following etiquette be adhered to by pupils involved in these sessions:
2. Dress appropriately- regular daytime clothing.
3. Make sure the child's name is registered for Zoom.
4. Wait in the lobby until you are admitted to the meeting.
5. Only children's names who are part of the class will be admitted to join the meeting from the lobby.
6. Be aware of your surroundings- Pick a room that is not a bedroom and does not have traffic passing through. Be mindful of noise from other people or pets.
7. Mute your microphone when you are not talking- only turn on the microphone if you are asked to speak. Muting the microphone when you are not speaking gives others the ability to chime in and share their thoughts without distraction or frustration.
8. Leave the keyboard alone- the sound of your typing is distracting.
9. Be respectful- teachers and pupils are real people who are affected by words that you say and write.
10. Using chat- do not use chat when the teacher is talking. Be respectful at all times when using chat. Remember that you are in a classroom, even if you are not wearing a uniform.
11. No food allowed- we do not want you dropping crumbs all over your keyboard!
12. Stay seated and stay present- do not leave the room or talk on your phone.
13. Be patient- this is new to a lot of people and it may take time to learn.
14. Do your best to engage in the meeting, be present and contribute when requested.

Appendix C:

Advice for Parents on ICT in the Home

During school hours, teachers will guide pupils toward appropriate materials on the internet. Outside school, parents or guardians should bear the same responsibility for such guidance as they normally would with other information sources, such as television, magazines etc. Parents or guardians should be aware that the internet service provider at home may not be filtered.

It is therefore important that these guidelines are followed:

- Discuss rules for using the internet with your children and decide together when, how long and what comprises appropriate use.
- Be aware of the sites your children are visiting and discuss with them what they are learning.
- Ensure that children do not give out personal identifying information on the internet such as a picture, full name, home address, email address, phone number, school name, financial information such as credit card or bank details or any personal codes issued by the school e.g. Seesaw access codes or Microsoft Office 365 account log in details.
- Encourage your children not to respond to any unwelcome, unpleasant, or abusive messages and to inform you if they receive any such messages or images.
- Reinforce with your child that if they do not know someone personally, they should not be communicating with them online.
- Ensure privacy settings for all messaging and social networking services are adequately set to prevent disclosure of detailed personal and/or location information.

Appropriate home use of the internet can be educationally beneficial and can make a useful contribution to home and schoolwork. It should however be supervised, and parents be aware that they are responsible for their children's use of the internet resources at home.
Consult the Webwise Parents Hub for information on online safety. https://www.webwise.ie/parents/

Page down for a sample of the following:
Letter to Parents
Responsible Internet Use Pupil Undertaking Form
Internet Permission Form
School Website Permission Form

Appendix D:

eLearning Code of Conduct

The following rules are in place to ensure the students in Scoil Bhríde get the best learning experience from the use of Microsoft Teams.

- I will be respectful of all participants.
- I will be kind, helpful and informative.
- I will respect others queries and questions.
- I will avoid the use of gifs and stickers in the class channels as they can clog up the feed.
- I will try my best to navigate Teams and will ask my teacher for help if I need it.
- I will remember that posts will be read by students, teachers, principal, and parents.
- I will keep my camera turned on when I am on a call with my teacher.
- I will <u>not</u> use the calls/video feature on teams to contact my classmates.
- I will <u>not</u> use the chat function to chat to another child (in my own class or another class). I will only communicate with my teacher on the chat function.
- I will <u>not</u> post any pictures other than those relevant to my schoolwork on Teams.
- I will <u>not</u> take pictures of or record any work online.

I agree to the above.

Child's name: _____

Appendix E:

OIDE Technology in Education: Content Filtering for Schools

Content filtering is an essential and integrated element of the broadband service that is provided to schools by the Schools Broadband Programme. The purpose of Content filtering is to ensure (in so far as possible) that inappropriate websites and content are not accessible from within schools. Within the content filtering service provided, schools are given a choice of six different levels of content filtering so that they can choose a level that best meets their particular situation, age group of students etc. Schools can choose from these six levels, and the chosen level of content filtering is implemented by the Schools Broadband team for the school. If schools subsequently want to change the level that is applied, they can do so by a formal written communication from the school to the Schools Broadband Service Desk, which is the single point of contact for all schools in relation to schools broadband. Content filtering systems classify websites into different 'categories', and these categories are used to control which category of website is allowed for schools on the different filtering levels. Level one is the most restrictive (as outlined below), while level six is the 'widest' level available as it allows access to websites such as you tube, personal blogging and social networking. The six levels are summarised below, all six levels block access to inappropriate material in categories such as pornography, violence etc.,

Level 1
This content filtering level allows access to a specific list of educational and related websites and other websites commonly used by schools. Level 1 is used by a very small number of schools, as it is generally perceived as being a little too restrictive by most schools.

Level 2
This level allows access to a wide range (i.e. millions) of educational and other websites but it blocks websites belonging to the 'games' category.

Level 3
This level is currently used by a majority of schools. It allows access to millions of websites including games but blocks 'YouTube', and blocks access to websites belonging to the 'personal websites' category and websites such as Facebook belonging to the 'Social Networking' category.

Level 4
This level allows access to the same websites as Level 3, but allows access to 'YouTube', which has become widely used in schools for teaching and learning in the last few years.

Level 5
This level allows access to the same websites as Level 4, but allows access to 'personal websites category', and other similar types of websites, such as blogs.

Level 6
This is the widest level of content filtering available. This level allows access to the same websites as Level 5, but allows access to Social Networking sites, such as 'facebook', and other similar social networking web sites.

Appendix F: Sample Letter to Parents

Insert Date

Dear Parent/Guardian,

As part of the school's education programme we offer pupils supervised access to the Internet. This will allow pupils vast educational opportunities by helping them for example, locate material for projects, communicate with students from different cultures, become independent in controlling their own research and become independent learners.

While we as educationalists recognise the value of the Internet as a resource, we must also acknowledge the potential risks to students. We feel that the answer is not to ban the use of the Internet in school but to teach pupils to recognise the risks and to become Internet Wise. We also allow limited access to 'YouTube' on a strictly supervised basis. This is to allow access to a huge range of educational material. The filter to prevent access to unsuitable material on YouTube is also in operation.

This process is the responsibility of the school and the parent/guardian.

For this reason, we have compiled a school policy on Internet safety. Parents must also set and convey standards of usage to their children.

It is important that you read the school's Internet Policy and sign the attached document.

There is also a document for pupils to sign. Parents should discuss this document with their children to ensure that they clearly understand the school rules with regard to Internet usage.

Mise le meas,

_____

Principal

Appendix G:

Responsible Internet Use
Pupil Undertaking

We use the School computers and Internet connection for learning.

These rules will help us to be fair to others and keep everyone safe.

I will ask permission before entering any website, unless my teacher has already approved that site

I will not bring external storage devices such as memory sticks/USB keys etc. into school without permission

I will not use email for personal reasons

I will only use email for school projects and with my teacher's permission

The messages I send will be polite and sensible

When sending e-mail, I will not give my home address or phone number or arrange to meet anyone

I will ask for permission before opening an e-mail or an e-mail attachment

I will not use internet chat rooms

If I see anything I am unhappy with or if I receive a message I do not like, I will tell a teacher immediately

I know that the school may check my computer files and may monitor the sites I visit

I understand that if I deliberately break these rules, I could be stopped from using the Internet and computers and my parents will be informed.

Signed: _____Pupil(s)

Signed: _____ Parent/Guardian

Date: _____

Appendix H:

Internet Permission Form

Name of Pupil(s): _____

Class(es): _____

As the parent or legal guardian of the above child, I have read the Internet Acceptable

Use Policy and grant permission for _____
(name(s): son/daughter) to access the Internet. I understand that school internet usage is for educational purposes only and that every reasonable precaution will be taken by the school to provide for online safety.

I accept my own responsibility for the education of my child(ren) on issues of Internet Responsibility and Safety.

I understand that having adhered to all the enclosed precautions the school cannot be held responsible if my child tries to access unsuitable material.

Signature: 1. _____ 2. _____

Parents/Legal Guardians

Date: _____

School Website

I understand that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the school's website. I understand and accept the terms of the Acceptable Usage Policy in relation to publishing pupils' work and photographs of school activities on the website.

Signature: 1. _____ 2. _____

Parents/Legal Guardians

Date: _____