E-Safety Policy
And
Acceptable Use Agreement

St. Francis of Assisi PS

Approved	May 2022
Review Date	Sept 2025

Background

ICT **-** The term, Information and Communications Technology (ICT) covers a range of resources from traditional computer-based technologies to the fast-evolving digital communication technologies.

Some of the Internet-based and electronic communications technologies which children are using, both inside and outside of the classroom, are:

- Websites
- Learning Platforms / Virtual Learning Environments (Google Classroom/ Seesaw)
- Email and Instant Messaging
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting - Skype/FaceTime/ Zoom/ Google Meet
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- IPads and other tablet devices with internet access

While these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with their use.

E-Safety

E-Safety encompasses internet technologies and electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- E-Safety concerns safeguarding children and young people in the digital world.
- E- Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more on education about the risks as well as the benefits so pupils can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

In St. Francis of Assisi P.S we understand our responsibility to educate pupils in E-Safety. We aim to teach children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The school's E-Safety policy will operate in conjunction with other policies including those for Remote Learning, Anti-Bullying, Safeguarding, Child Protection, Image Consent Form and Security.

Risks and Responses

The Internet is an exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key Concerns are:

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons

In our school children will be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information (e.g. send inappropriate photographs) it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet.

Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.

Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

In our school children will be taught:-

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Cyber Bullying

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites. If it takes place within school, cyberbullying will be dealt with in line with the school's overall anti-bullying policy, discipline policy and pastoral services.

Good Habits

In our school children will be taught:

- If they feel they are being bullied by e-mail, through social networking sites, text or online they should always tell someone they trust.
- Not to reply to bullying, threatening text messages or e-mails as this could make things worse.

- Not to send or forward abusive texts or e-mails or images to anyone.
- Keep abusive messages as evidence.
- Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.
- Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school
- We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

E-Safety depends on effective practice on a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of E-Safety policy in both administration and curriculum, including secure network and design
- Safe and secure broadband from the provider including effective management of content filtering
- National Education Network standards and specifications

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. Mr Sloan has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

The Principal/ICT Co-ordinator update Senior Management and Governors with regard to E-Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the E-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The E-Safety Policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on E-Safety issues through the co-ordinator at staff meetings or planned CPD sessions.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

- New staff members receive information on the school's E-Safety Policy and Acceptable Use Agreement as part of their induction.
- All teachers are encouraged to incorporate E-Safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

Parents/carers have an important role to play in promoting E-Safety. We encourage all parents/carers to become involved in E-Safety discussions and activities with their child.

- The school website contains links to sites such as CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page which parents can use with their children
- The school communicates relevant E-Safety information through parents' evenings/newsletters and the school website.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement with their child.
- Parents/carers are required to give written consent to images of their child being taken/used on the school website.

Parents are reminded regularly that it is important to promote E-Safety in the home and to monitor Internet use. The following guidelines are provided:

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips and the "Click Clever, Click Safe" code
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.

- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- Teachers will plan for and provide opportunities across the curriculum for children to develop their E-Safety skills.

- Educating children on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise, and as part of the E-Safety curriculum.

- Children are made aware of the impact of online bullying and know how to seek help if these issues affect them. Children are also made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service using a Websense filtering solution.

- Websense assesses all websites based on their content and adds them to a category. (Green – available, Red – unavailable) All users are given access to a core group of green sites. The school has the facility to customise security options where need arises. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.
- No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult.

- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

- Children are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Children are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. They will be taught to be "Click Clever, Click Safe":

  Zip it (never give personal data over the internet)
  Block it (block people you don't know)
  Flag it (if you see something you don't like flag it up with someone you trust).

Email:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Forwarding chain letters is forbidden.
- Sending or displaying insulting or offensive messages/pictures is forbidden.
- Using obscene language is forbidden

Social Networking:

- Through the C2k system our school currently blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Portable Technologies:

- The use of portable devices such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile phones during class.
- Staff should not use personal mobile phones during designated teaching sessions.

iPads

iPads are used for digital storytelling, internet research, and to support learning and teaching across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet Wise and apply the Internet safety rules. They will not be allowed to use iPads to:

- Take photos of pupils/staff without permission or direction from the teacher.
- Take videos of pupils/staff without permission or direction from the teacher.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Please see Remote Learning Policy for updated guidelines on the use of video-conferencing.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's E-Safety rules. These E-Safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised..
- All parents/guardians will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's E-Safety rules and within the constraints detailed in the school's E-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password. They are encouraged to keep details of usernames and passwords private.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling E-Safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the E-Safety incident logbook.
- As part of the Acceptable Use Agreement children will know that if they deliberately break the rules they could be stopped from using the Internet/E-mail and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Complaints regarding cyberbullying will be dealt with in line with the school Anti-Bullying Policy.
- Pupils and parents will be informed of the complaints' procedure.
- Any complaint about staff misuse must be referred to the Principal and governors.

Communicating the Policy:

Introducing the E-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored**.**

.

Staff and the E-Safety Policy:

- All staff will be involved in discussions regarding E-Safety and will have a copy of the E-Safety Policy.
- Staff will be aware that Internet use can be monitored and traced to the individual. Professional conduct is essential.
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone where contact with pupils or parents is required

Staff should follow the guidelines below:

- Never communicate with pupils outside of school via social networking sites and chat rooms.
- Never respond to informal, social texts from pupils
- Never use personal technology to take images or videos of children

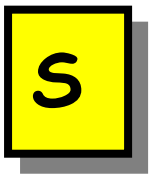
Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

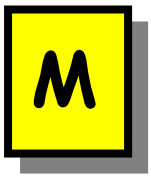
This policy is the governors' responsibility and they will review its effectiveness annually. They will do this through liaison with the ICT Co-ordinator and the Designated Child Protection Co-ordinator.

Safety Rules for Children

Follow These SMART TIPS



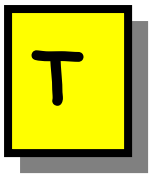
Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Proctection Committee

An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents/guardians are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks or mobile devices from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.

I

- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
- I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/carers will be informed.

St. Francis of Assisi Primary School

Acceptable Use Agreement
For Pupils

Please discuss the Acceptable Use rules with your child and then complete and return this form to your child's class teacher

Pupil's Name		**Class Teacher**	
As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
Pupil Name (print)			
Pupil Signature		**Date**	

Parent's Name			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.			
Parent's Name (print)			
Parent's Signature		**Date**	

St. Francis of Assisi Primary School
Acceptable Use Agreement
For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's E-Safety Policy has been drawn up to protect all parties – the children, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- Internet use should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised C2K account and password, which should not be made available to any other person
- The C2k email account should be used for professional purposes.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access or send inappropriate materials such as pornographic, racist or offensive material is forbidden
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden

Name		
Date		**Signed**

St Francis of Assisi Primary School
E Safety Audit

This quick self-audit will help the ICT Team assess whether the E safety basics are in place.

Has the school an E-Safety Policy that complies with DENI guidelines?	Yes
Date of latest update:	March 2022
The Policy was agreed by governors on:	May 2022
The Policy is available for staff at:	Document on Staff Files.
Available to Parents at:	Policy available on school website. Information Leaflet given to parents at the beginning of the school year.
The Designated Child Protection Teachers are:	Mrs M O Malley S Bean Uí Thuathail
The E-Safety Coordinator is:	Mr Conor Sloan
The E-Safety Governor is:	Mrs Leah McAleavey
Has E-Safety training been provided for both pupils and staff?	Yes
Do all staff sign an Acceptable Use Agreement on appointment?	Yes
Do all pupils/ parents sign Acceptable Use Agreement?	Yes
Have school E-Safety rules been set up for pupils?	Yes
Are those rules displayed in all rooms with computers/ iPads?	TBC
Internet access is provided by an approved educational internet service provider and complies with DENI requirements for safe and secure access?	Yes- C2k
Is personal data collected, stored and used according to the principles of the Data Protection Act 2018?	Yes

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Broadband monitoring logs of internet activity
- ICT Coordinator (E safety Officer) and ICT Team members will meet regularly to review monitoring

Lending IT Devices to Pupils – IT Equipment Loan Agreement

IT Equipment Loan Agreement

DETAILS TO BE COMPLETED BY SCHOOL CONTACT:

Named Pupil/s (Name and address)):

Responsible Person – (Parent/Carer's Name & Address email contact telephone number):

School (name and address):

St Francis of Assisi

School Contact (name / email address/telephone number):

Mr Conor Sloan

csloan622@c2kni.net

Details of specific IT Equipment

IT Equipment Name:

IT Equipment Serial Number:

TERMS AND CONDITIONS COVERING THE LOAN OF THE IT EQUIPMENT

The School has agreed that that the identified IT Equipment as detailed in the attached IT Equipment Loan Record will be loaned to your child for a period initially up to (DATE TBC). This loan is subject to review on a regular basis, and can be withdrawn at any time.The School also reserves the right the substitute the IT Equipment at any time if necessary.

As a parent/guardian/carer of a pupil to whom IT Equipment has been loaned you have read and agreed to the following terms and conditions:

1. The IT Equipment remains the property of the School and has been loaned for the sole purpose of assisting in the delivery of the School curriculum to the Named Pupil or pupils.

2. When the term of this Agreement ends you as the Responsible person will return the IT Equipment to the School Contact by a specified time and in a specified manner.

3. You should return the IT Equipment to the School Contact in the same condition as you received it excepting for reasonable wear and tear.

4. You should return the IT equipment in person so that it can be inspected by the School for any visible damage.

5. Any change of home address by the Named Pupil must be notified to the School Contact without delay.

6. The IT Equipment and the connectivity equipment must not be used for any illegal and/or anti-social purpose.

7. The IT Equipment may be used by other family members whilst supporting the named Pupil's education but must not be used for any other activities unless otherwise approved by the School. On no account must the IT Equipment be used by anyone else or be allowed to go out of the possession of the Responsible Person or Named Pupil.

8. You must ensure that:

    a. The Named Pupil and any permitted family user supporting the named Pupil's education treats the IT Equipment with appropriate care and the IT Equipment is maintained in good condition.

    b. The IT Equipment is not left unattended without being stored securely.

    c. The Named Pupil and any permitted family user avoids food and drink near the IT Equipment.

9. The School cannot accept responsibility for the loss of work in the event of the IT Equipment malfunctioning.

10. It is the responsibility of the Named Pupil to back-up their work regularly.

11. You must only use software licensed, authorised or installed by the School or C2k.

12. Anti-Virus software installed by the School or C2k must not be uninstalled.

13. There may be occasions when the School will need the IT Equipment to be returned to the School for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the IT Equipment. The School cannot be held responsible for the loss or damage of any data on the IT Equipment during this process the IT Equipment must be returned to the School without unnecessary delay by the Responsible Person as and when requested.

14. During the upgrade and maintenance process, technical members of School staff may view data or programmes on the IT Equipment. You will be held responsible for ensuring use of the IT Equipment is in accordance with the School's acceptable use policy at this point. You may want to remove personal data from the IT Equipment before its return.

15. All technical support and maintenance issues must be raised with the School Contact initially without unnecessary delay.

16. If the IT Equipment is stolen you must immediately report it to the police and get a crime reference number. You must immediately report this to the School Contact.

17. If the IT Equipment is accidentally damaged, you must immediately contact the School Contact and the equipment presented for examination. You must not arrange to have repairs undertaken elsewhere. The School will do its best to repair the damage. If this is not possible, replacement will be considered on a case by case basis. If this damage is not the result of normal wear and tear, you will be liable to reimburse the School for any reasonable repairs and labour costs.

18. You must ensure that that the external face of the equipment provided is not decorated or changed in any way, including affixing stickers.

19. Reasonable health and safety precautions should be taken when using the IT Equipment. The School is not responsible or any damage to person or property resulting from the IT Equipment loaned.

20. The School is not responsible for any costs resulting from the use of the IT Equipment and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.

21. The School is not responsible for any broadband charges incurred by the Named Pupil or any permitted family user of the IT Equipment accessing the internet from any site other than school premises are not chargeable to the school.

22. You will ensure that any internet access using of the IT Equipment at home is for an appropriate educational purpose.

23. All information and supporting documentation supplied by you with this Agreement will be used for the sole purpose of providing the IT equipment. Your IT Loan

Agreement and related information, will be held and maintained by the School in accordance with the provisions of Data Protection Legislation. The data will not be passed to any other third party without your consent, except when the School is required to do so by law.

24. By accepting the IT Equipment you are confirming that you have read and agree to adhere to current School policies regarding the following: Acceptable Use, Data Protection, Computer Misuse and Health and Safety which are attached to this Agreement.

The School reserves the right not to replace a lost or damaged device.

Responsible Person (Parent/Guardian/Carer) Agreement:

I have read and agree to be bound by the terms and conditions set out above.

Name of parent / Guardian / Carer: ……

Signature parent/ Guardian / Carer: ……

Date: ……..