# Kingsmills Primary School

**Play, discover, learn, grow'**

# Online Safety

Reviewed: Sept 2020

Review Date: Sept 2021

| | |
|---|---|
| | |
| Chair of Board of Governors | Date: |
| | |
| Principal | Date: |

# Contents

# Online Safety Policy

## Introduction

Kingsmill's Primary School Online Safety Policy reflects the importance we place on the safe use of information systems and electronic communications. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. Online safety encompasses not only Internet technologies but also 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 responsibility of using information technology.

Whilst 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 the use of Internet Technologies.

## Online Safety:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use technologies in a positive way;
- is less about restriction and focuses on educating children about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting children and young people to develop safer online behaviours both in and out of school;
- prepares pupils to recognise unsafe situations and how to respond to risks appropriately.

In Kingsmill's Primary School we understand the responsibility to educate our pupils in Online Safety issues. We aim to teach them 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 has a duty to provide pupils with quality internet access as part of their learning experience. The internet is part of the statutory curriculum and an entitlement for pupils as part of their learning experience. It is used in this school to raise educational standards, promote pupil achievement and as a necessary tool for staff to support their professional work. The internet also enhances the school's management information and business administration systems.

This policy operates in conjunction with other school policies including Positive Behaviour, Child Protection/Safeguarding Children and Anti-Bullying. Online Safety must be built into the delivery of the curriculum.

Online Safety in Kingsmill's Primary School depends on effective practice at several levels:

- responsible ICT use by all staff and students, encouraged by education and made explicit through policies.
- sound implementation of the online safety policy within education.
- continuous use of Securus to check students keystrokes and screen grabs and evaluation using 360 Safe Tool.
- safe and secure internet provision by C2K.

**The Internet**

The Internet is a unique and 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
Children should 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 or
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information 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.

Children should 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.

**Excessive Commercialism**

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet Safety. Teachers, pupils and parents must be vigilant.

**Aims**

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.
- Take the necessary measures to block and delete accounts, messages and people.

**Roles and Responsibilities**

Online 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. The ICT Co-ordinator/Team has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

The Principal/ICT Co-ordinator have the responsibility to update the Senior Leadership Team and Governors with regard to E-Safety and all governors should understand 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 and pupils, is to protect the interests and safety of the whole school community.

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

**The Board of Governors**

- Are responsible for the approval of this policy and reviewing its effectiveness. The Governors should receive regular information about Online Safety incidents and monitoring reports.

**E-Safety Skills' Development for Staff**

- All staff will be given the School E-Safety Policy and its application and importance explained.
- All staff will receive regular information and training on E-Safety issues through the co-ordinator at staff meetings.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- 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 will receive a copy of the E-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- All staff are encouraged to incorporate E-Safety into their activities and awareness within their lessons.

**E-Safety Information for Parents/Carers**

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and/or used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate and promote relevant E-Safety information through newsletters and the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

Parents should remember that it is important to promote E-Safety in the home and to monitor Internet use.

- Keep the computer/iPad/tablet 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/games consoles/tablets.
- 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.
- 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 online may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- 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.
- Keep passwords private at all times and do not allow their children access to these.

**Teaching and Learning**

**Internet use:**

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.
- Key E-Safety messages will be reinforced annually through an assembly and Safer Internet Week.
- The school will liaise with local organisations to establish a theme or common approach to E-Safety in the form of a workshop/talk. This may take place in Key Stages or as a whole school approach.
- Educating pupils 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.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, Safeguarding Team, Class Teacher/trusted member of staff.
- E-Safety is a focus in all relevant areas of the curriculum.
- The school Internet access is filtered through the C2k managed service. 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. Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Pupils will be helped to understand and act in accordance with the ICT Acceptable Usage Agreement of Pupils.
- Pupils will be 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.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- 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.
- When using digital images, pupils are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff act as good role models in their own use of ICT.

**E-mail:**

- Pupils may only use approved e-mail accounts in school, e.g. 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.
- The forwarding of chain mail is not permitted.

**Social Networking:**

- The school network system will block 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.
- Pupils will be advised not to place personal photos on any social network space. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school.
- Our pupils are encouraged to report any incidents of cyber bullying to the school. A record of cyber bullying incidents will be kept to monitor and support our sanctions.
- Pupils will be advised that sending abusive messages or images in any online format will be considered as bullying and will be dealt with accordingly.
- If staff or pupils discover unsuitable sites, the URL must be reported to a member of the ICT Team.
- School staff will not add children as 'friends' if they use these sites.

**Mobile Technologies:**

**Staff:**

- The use of portable media 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' photographs on memory sticks.
- Staff USB pens carrying personal information should be password protected.
- Staff should not use personal mobile phones during designated teaching sessions, they should be on silent, placed away from view or switched off.
- If there are extreme circumstances the member of staff will have made the Principal aware of this and have their phone on in case of having to receive an emergency call.
- Use of phones should be limited to non-teaching time, when no children are present.
- Phones will never be used to take photographs of children or to store their personal information.
- A mobile will be carried to sporting fixtures, educational visits away from school for contacting parents in the event of an emergency.

**Pupils:**

- Pupils are not allowed to use personal mobile devices/phones in school.
- The school takes no responsibility for mobile phones. They are brought to school entirely at their own risk.
- Where a pupil is found with a mobile phone during the school day the phone will be taken from the pupil and stored in the school office to the end of the school day. The pupil can collect their phone at the end of the school day and their parent/guardian contacted.
- Phones must never be used to photograph other children within school.
- If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the pupil, in the presence of a member of the safeguarding team has removed the images. A member of the safeguarding team will contact a parent/guardian before asking the child to delete material from their phone.

**Managing Videoconferencing:**

- Videoconferencing will be via the C2k network to ensure quality of service and security. The school will use Ultra Collaborate, Teams, Zoom and Google Classroom during times of home schooling.
- Videoconferencing will be appropriately supervised by parents when in use.

**Publishing Pupils' Images and Work**

The school Website's address is www.kingsmillsps.co.uk. As our website continues to grow, we intend to develop the existing gallery/articles featuring both pupils work and the pupils themselves engaged in a variety of noteworthy activities. When posting photographs to the site we will ensure that:

- 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
- Pupils' full names will not be used on the School Website in association with photographs.
- Teachers will endeavour to take pictures of groups or group activities; however individual pictures will be used from time to time.
- Staff are allowed to take digital/video images to support educational purposes following the online safety policy. Images should only be taken on school equipment, e.g. school cameras, iPads.
- Any member of the ICT Team has the authority to refuse, withdraw or delete an inappropriate image or article from the school website. The Principal will also have the ability to do this.
- Pupil's work will be displayed on our school website on occasions.
- Any article/image on our website remains the property of our school.

**Policy Decisions:**

**Authorising Internet access:**

All staff must read and sign the 'Acceptable Use Agreement for Staff' before using any school ICT resource.

- All access to the internet will be supervised.
- The school will take all responsible precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Therefore, the school cannot accept liability for the material accessed or any consequences resulting from Internet use.
- Complaints of Internet misuse will be dealt with by the Safeguarding Team in school.
- Any complaint about staff misuse must be referred to the Principal.
- E-Safety rules will be posted in classrooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

**Handling Online Safety Complaints:**

- Complaints of Internet misuse will be dealt with by the Safeguarding Team who will inform the ICT Co-ordinator/Team if and when appropriate.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator in the online safety logbook and reported to Safeguarding Team/SLT/Principal.
- Any complaint about staff misuse must be referred to the Principal.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints' procedure.

**Communicating the Policy:**

**Introducing the Online Safety Policy to pupils**

- Online Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. The SMART rules will be continually reinforced throughout the school year in all aspects of the curriculum when using the Internet. Specific lessons on Online Safety will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times.

- Pupils will be informed that network and Internet use will be monitored**.**

**Staff and the Online Safety Policy:**

- All staff will be given the Online Safety Policy and its importance explained.

- Any information downloaded must be respectful of copyright, property rights and privacy.

- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct are essential.

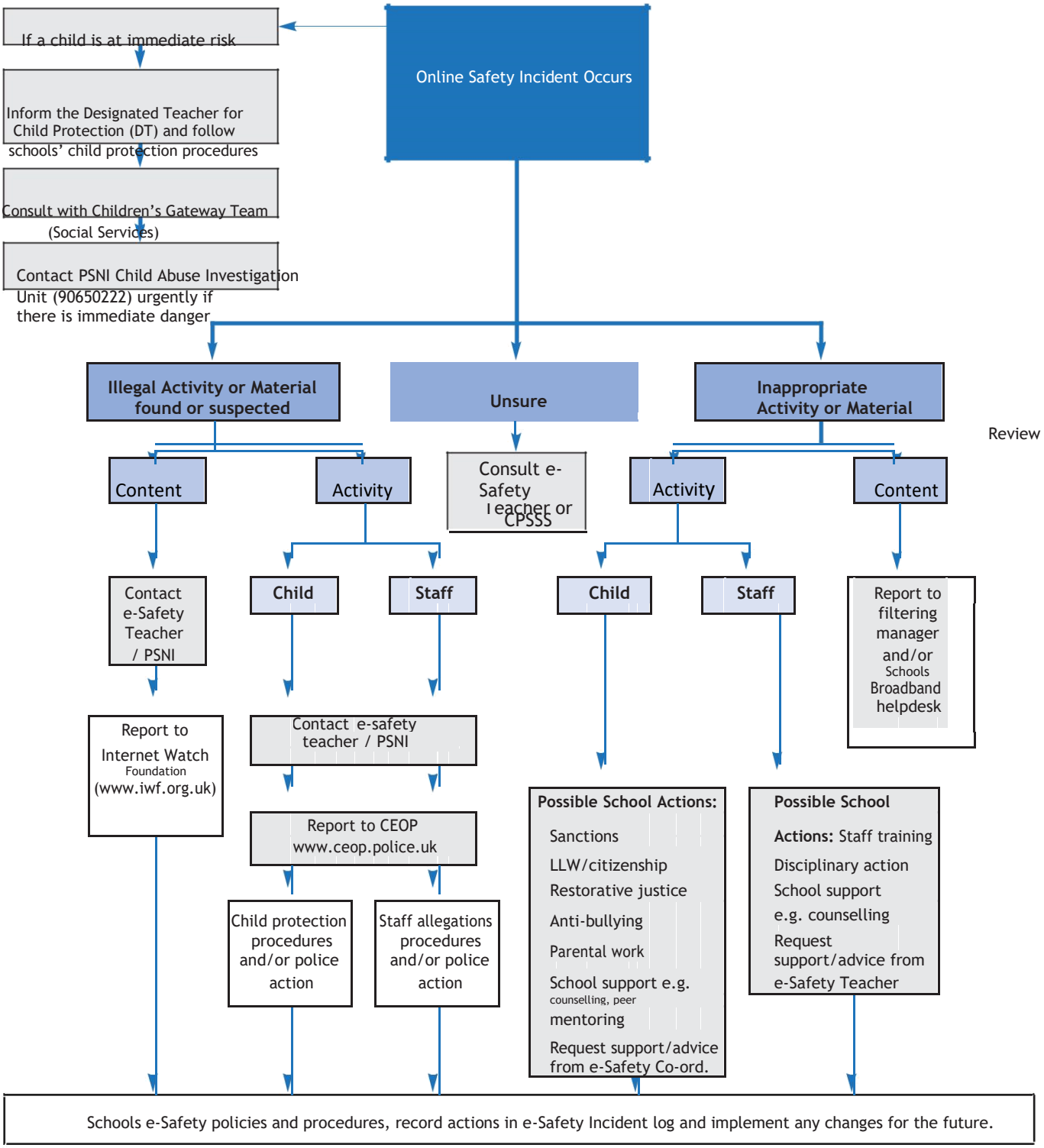
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

**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/Team.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator/Team and Senior Leadership Team.

# Response to an Incident of Concern




Schools Designated Teacher for Child Protection: Mrs Scroggie

School's E-Safety Co-ordinator: Mrs Courtney

E-Safety/Child Protection Governor: Mr Taylor

PSNI Child Abuse Investigation Unit: 02890 259299

Gateway Team (Social Services): 208 9598 5590

P5-P7

# ALWAYS BE SAFE – FOLLOW THE SMART RULES!

## Follow These SMART TIPS

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

**M** **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.

**A** **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.

**R** **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!

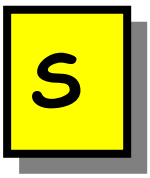
**T** **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

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

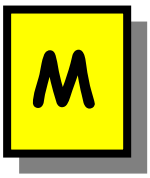
P3-P4

# ALWAYS BE SAFE – FOLLOW THE SMART RULES!

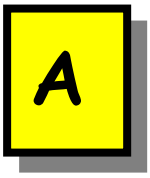
## Follow These SMART TIPS



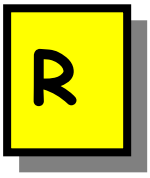

**Secret -** Always keep your name, address, and password private.



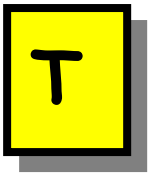

**Make** sure you tell your parent or teacher if someone wants to talk to you when you are online.




**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.




**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 Protection Committees

**P5-P7**

# 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 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/laptops/iPads.
- 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 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 understand that if I deliberately break these rules, I could be stopped from using the Internet/E-mail and my parents/carer will be informed.

**Signed by Child:** _____

**Signed by Parent/Guardian:** _____

**Date:** _____

**P3-P4**

# 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 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 open 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 activities 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 I must look after and take care of the school computer, laptop or iPad I am using.
- 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 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 and may monitor the Internet sites that I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet and my parents/carer will be informed.

**Signed by Child:** _____

**Signed by Parent/Guardian:** _____

**Date:** _____

**Foundation Stage**

## An Acceptable Use of the Internet

# Think then Click

These rules help us to stay safe on the Internet

**I will only use the computer when my teacher allows me.**

**I will only use the internet when an adult is with me.**

**I can click on the buttons or links when I know what they do.**

**I will always ask if I get lost on the Internet.**

**I understand that the school can check my files on the computer.**

**I know that if I break the rule's, I might not be allowed to use the computer.**

**An adult has explained the rules for Safe Use of the Internet to me.**

**Signed by Child:** _____

**Signed by Parent/Guardian:** _____

**Date:** _____

# 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 Internet Access Policy has been drawn up to protect all parties – the students, 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.

- I understand that all Internet activity should be appropriate to staff professional activity or the pupils' education.
- I will not disclose any password or security information to anyone other than an appropriate system manager.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- I understand that users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- I will not install any software or hardware without permission.
- Copyright of materials must be respected.
- I understand that staff members may use school camera equipment on field trips; any images should be appropriately transferred back to a centralised area in the staff public folder.
- I understand that the use of camera phones will not be permitted by pupils or staff.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- 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 for personal financial gain, gambling, political purposes or advertising is forbidden.
- I will not use the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- I will report any incidents of concern regarding children's safety to the school E-Safety Coordinator or the Designated Child Protection Teacher.
- I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

| **Name** | | |
|---|---|---|
| **Date** | | **Signed** |

# iPad Acceptable Use Policy

At Kingsmills Primary School I-Pads 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 I-Pads, children will be reminded to be Internet Wise and apply the online safety rules.

The policies, procedures and information within this document apply to all I-Pads or any other IT handheld device used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

## Users' Responsibilities (including members of staff)

- Users must use protective covers/cases for their I-Pad.
- The I-Pad screen is made of glass and therefore is subject to cracking and breaking if misused: neither drop nor place heavy objects (books, laptops, etc.) on top of the I-Pad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the I-Pad screen.
- Do not subject the I-Pad to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that persons' consent.
- The I-Pad is subject to routine monitoring by Kingsmills Primary School.
- Devices must be surrendered immediately upon request by any member of staff.

## Safeguarding and Maintaining as an Academic Tool

- I-Pad batteries are required to be charged and be ready to use in school.
- Syncing the I-Pad to iTunes or iCloud will be maintained by the school Principal.
- Items deleted from the I-Pad cannot be recovered.
- Memory space is limited. Deletion of photos and videos will happen periodically by the Principal, ICT Co-Ordinator or Staff members.
- I-Pads must always be returned after use and are never to be taken home by children.
- All staff I-Pads must be in school each day.
- If an I-Pad is found unattended, it should be given to the nearest member of staff.

## Lost, Damaged or Stolen I-Pad

- If the I-Pad is lost, stolen, or damaged, Mrs Harrison or Mrs Courtney must be notified immediately.

- I-Pads that are believed to be stolen can be tracked through iCloud.

**Prohibited Uses (not exclusive):**

- Accessing Inappropriate Materials – All material on the I-Pad must adhere to the ICT Policy.
- Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Violating Copyrights – Pupils are not allowed to have music and install apps on their I-Pad. This is the responsibility of the Principal.
- Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate photographs or videos, nor will it be used to embarrass anyone in any way.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; the Principal.
- Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.
- Misuse of Passwords, Codes or other Unauthorized Access: Only the Principal has access to the I-Pads' passcodes.
- Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Jailbreaking – Jailbreaking is the process which removes any limitations placed on the I-Pad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
- Inappropriate media may not be used as a screensaver or background photo.
- Kingsmills Primary School reserves the right to confiscate and search an I-Pad to ensure compliance with this Responsible Use Policy.

# Kingsmills Primary School iPad Pupil Pledge

In order to ensure that the iPads in our school are used correctly all pupils and parents are required to sign the agreement below.

Pupil Pledge for iPad Use

1. I will take good care of any iPad I use.
2. I will know where the iPad is at all times when I am using it.
3. I will keep food and drinks away from the iPad.
4. I will protect the iPad by only carrying it whilst it is in a case.
5. I will use the iPad in ways that are appropriate.
6. I understand that the iPads are subject to inspection at any time without notice.
7. I will only photograph people with their permission.
8. I will only use the camera or the microphone when my teachers tell me to.
9. I will never share any images or movies of people in a public space on the Internet, unless I I am asked to do so by my teacher.
10. I will not hide any iPad so others cannot use it.
11. I agree to abide by the statements of this iPad acceptable use policy

I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.

Name of child _____

Signature of child _____

Signature of Parent/Guardian _____

Date _____

# Password Protection Policy

## Rationale

Kingsmill's Primary School recognises the importance of security when using digital technology in school. We are committed to ensuring staff and pupils are equipped with the knowledge to protect themselves and others against unauthorised access to school systems.

## Introduction

The school will be responsible for ensuring that the school network infrastructure (C2k) is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission.
- Access to personal data is securely controlled in line with the school's personal data policy.

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems.

## Passwords

### Pupils

All pupils are provided with an individual login username and password that they should not reveal to anyone. Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.

With regard to password use on the network infrastructure (C2k) the following security principles should be applied by all staff and pupils.

- Passwords should not be obvious. For example, words such the user's name or the name of a favourite pop group should not be used.
- Passwords should be at least eight characters long.
- Passwords should contain upper- and lower-case letters as well as numbers and special characters.
- Passwords should remain confidential and never be written down.
- Passwords should be changed every 120 days and C2k will prompt the user to do so.
- Passwords cannot be reset within 2 days by the User. *However, individual pupil passwords can be reset by the C2k Manager.*

If a pupil believes their password is known by someone else, then they should see a member of staff or the ICT co-ordinator. They will be prompted to use **CTRL ALT DEL** to reset their password from the

desktop and a message will be displayed to alert the user if any of the rules discussed above have been broken.

**Staff**

Staff users are provided with an individual login username and password, which they are encouraged to change periodically. Personal staff login details should not be shared with pupils. Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network. Furthermore, staff should be aware that they can change their password outside of school by visiting this website - https://services.c2kni.net/ums/

Should a teacher user forget their password they must request the school C2k Administrator or C2k Manager to reset their password. Only the Administrator or Manager can reset Staff passwords.

**Training / Awareness**

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users.

Members of staff will be made aware of the school's password policy:

- At induction.
- Through the school's e-safety policy and password protection policy.
- Through the Acceptable Use Agreement for Staff.

Pupils will be made aware of the school's password policy:

- During ICT, PDMU and /or e-safety lessons (Children will be given opportunities to explore and discuss various safety/security scenarios through recommended sites such as 'Think u know' and 'Childnet')
- Through the Acceptable Use Agreement for Pupils.