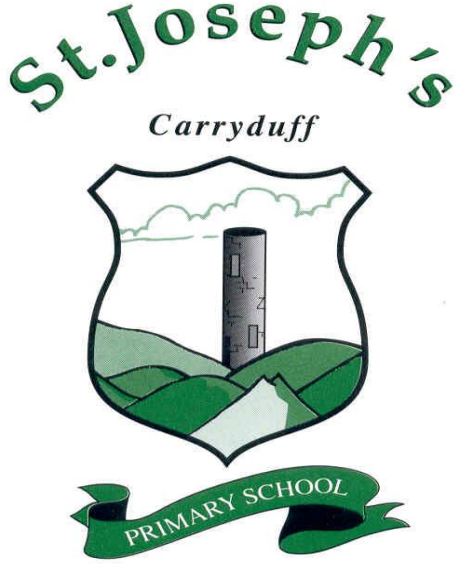


Policy for e- Safety and Acceptable Use of the Internet and Digital Technologies

September 2024

Introduction

In today's rapidly changing world, it is important to ensure that safe, responsible, acceptable and effective use is made of the internet and other digital technologies by the children in our care. It should be recognized that children have access to a range of digital technologies including web-based and mobile learning through devices such as iPads. Currently the internet technologies children are using, both inside and outside the classroom, include:

-Websites

-Learning platforms and Virtual Learning Environments

-Email and instant messaging

-Chat rooms and social networking

-Blogs and wikis

-Podcasting

-Video broadcasting

-Music downloading

-Gaming

-iPads

-Mobile/Smart phones with text, video and/or web functionality

-Other mobile devices with web functionality

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 online 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.
- "Stranger Danger" applies to the people they encounter through the internet.
- They should never give out personal details.
- They should never meet alone with anyone contacted via the internet.
- 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.
- To express views, e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.
- Containing misleading and inaccurate information, e.g. some use the web to promote activities which are harmful.

Children should be taught:

- That information on the Internet is not always accurate or true.
- That they should 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.

Roles and Responsibilities

As eSafety 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 eLearning Co-ordinator to keep abreast of current esafety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The Principal has responsibility for leading and monitoring the implementation of esafety throughout the school. The Principal/eLearning Co-ordinator update the School Leadership Team and Governors with regard to esafety and all governors have an understanding of the issues in relation to 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 and used in conjunction with other school policies including those for UICT,

Behaviour, Health and Safety, Child Protection, and Anti-bullying. This policy should not be seen as exclusive.

It has been agreed by the School Leadership Team, staff and approved by the Board of Governors. Pupils and parents have also been consulted. The eSafety policy and its implementation will be reviewed annually.

eSafety Skills Development for Staff

All staff receive regular information and training on eSafety issues through the eLearning Co-ordinator. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety 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 Acceptable Use Agreement as part of their induction. All staff are encouraged to incorporate eSafety activities and awareness within their lessons, as stipulated in the Using ICT guidelines.

eSafety Information for Parents/Guardians

Parents/Guardians are asked to read through and accept the terms of the Acceptable Use Policy on behalf of their child. Parents/Guardians are required to make a decision as to whether they consent to images of their child being taken/used on the school website. The school website contains useful information and links to sites like CEOP's, ThinkUKnow, and the CBBC Web Stay Safe page. The school will communicate relevant eSafety information through newsletter and the school website. Parents should remember that it is important to promote eSafety in the home and to monitor Internet use there. Guidelines include:

- 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 iPads and 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 (see later)
- 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

Why is Internet access important?

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. The benefits to the school are:

- Access to world-wide educational resources including museums and art galleries;
- Information and cultural exchanges between students world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for pupils and staff;
- Staff professional development - access to educational materials and good curriculum practice;
- Communication with the advisory and support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the relevant outside agencies;

Internet Use

Teachers, parents and pupils need to develop good practice in using the Internet as a tool for teaching and learning. The school will plan and provide opportunities within a range of curriculum areas to teach esafety. Educating children on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and formally as part of the esafety curriculum set out as part of the UICT guidelines. Pupils are also 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/guardian, teacher/trusted member of staff, or an organization such as CEOP. The school internet access is filtered through the C2K Managed Service. Access to the internet via the C2K Education network is fully auditable and reports are available to the school principal.

No filtering service is 100% effective therefore pupils will be informed that their use of the Internet will be supervised and monitored appropriately. Pupils will be taught what internet use is acceptable and what is not and will be given clear objectives for Internet use. Pupils will be educated in the effective use of Internet for research,

including the skills of knowledge location, retrieval and evaluation. They will be taught to acknowledge the source of information when using Internet material for their own use**.**

Children will be taught to be Internet wise and are made aware of Internet Safety Rules. They will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Internet access will be planned to enrich and extend learning activities and aimless surfing is not permitted. Children are taught to use the Internet as part of a planned teaching activity. Access levels will be reviewed to reflect the curriculum requirement.

E-mail:

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. The forwarding of chain mail is not permitted.

Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher and are always part of a planned and agreed learning activity. Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper;

Social Media:

Chat rooms, blogs and other social networking sites are blocked by the C2K filters so pupils do not have access to them in the school environment. Whilst we accept that parents are responsible for their children's use of social media outside school, pupils and parents will be advised that the use of social network spaces is inappropriate for primary aged pupils. **Parents should be aware that social networking sites such as Facebook, Snapchat, Twitter, Instagram and Pinterest restrict legitimate access to those of at least 13 years of age and, as such, should not be accessed by primary aged children.**

However, we are aware that some pupils will still use social media. Therefore, an increasingly important part of our safeguarding will relate to educating pupils on the safe and responsible use of social media. It is also important that all adult members of the school community (i.e. staff, parents, governors and all regular visitors to the school) model good practice and set an example for the children in their use of social media. Therefore, we expect that all member of the school community will adhere to the Code of Conduct regarding the Use of Social Media set out below:

- Confidential information including personal details about any member of the school community which may identify them or their location should not be posted online.
- profiles on social media sites should be set to maximum privacy to ensure access is denied to unknown individuals.
- treat other members of the school community with respect and ensure that comments are supportive, fair and positive
- comments should not be derogatory, rude, threatening or inappropriate
- Offensive language should not be used at any time
- Images of other children completing activities in school should not be posted on social media by parents or children without the consent of the parents of those whose images are to be displayed.
- Report any incidents of cyber bullying and/or any misuse of mobile phones/websites/email to a member of staff immediately
- staff or volunteers working in school will not add children as "friends" nor will they use social media to communicate directly with children who attend the school
- the school's name, logo or documents should not be posted online without the permission of the Principal
- any information which could potentially compromise the security of the school site should not be posted online
- parents are responsible for their children's use of social media outside of school. They should be aware of the age restrictions regarding particular forms of social media, for example, Snapchat, Instagram, Facebook and Whatsapp
- Comments which could result in reputational damage to the school or individual members of the school community or, which could be construed as being defamatory, should not be made online

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's anti-bullying and Child Protection procedures.

Mobile Technologies e.g. iPad:

When using iPads all pupils will be expected to follow the terms of this eSafety policy and other school policies. 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' personal data and photographs on memory sticks. Pupils are not allowed to use personal mobile devices/phones in school. Staff should not use personal mobile phones during designated teaching sessions.

Managing Online Learning including Video-conferencing during a Period of School Closure:

During any periods of prolonged school closure staff will use the C2K network to conduct teaching and learning remotely.

Remote learning will be conducted through Google Classroom and other C2K supported platforms. Seesaw will be used with Nursery children.

Pupils will be provided with their own unique usernames and passwords and access to the virtual classroom will be restricted to the pupils or their parents. Parents will be required to use a recognised email address and identify themselves as required.

Using these online tools, teachers will be able to maintain continuity in teaching and learning. This will include:

- Sharing teaching activities and support materials for completion by the pupils
- Using online functions to enable the provision of feedback to pupils on their work
- Encouraging peer evaluation of work which is moderated within the online classroom
- Providing opportunities for pupils to collaborate on shared documents e.g. presentations and research projects
- Sharing pupils' work within the Google Classroom
- Accessing content and activities to increase pupil engagement e.g. News Desk

Our remote teaching and learning will be underpinned by the following principles:

- Online teaching is an extension of the classroom and the Acceptable Use Policy will apply to all online teaching and learning activities
- Staff will avoid the use of personal mobile phones as far as possible. In the limited circumstances where staff need to contact a pupil using a personal phone, this will be agreed by the Principal/Vice-Principal.
- Staff will use their C2K email accounts and will avoid using personal accounts if contacting children or their parents
- All conventional professional teaching norms and standards will apply to online learning
- By using C2K platforms, teachers will be able to maintain full control of the audio and video content that is shared on the platform
- Staff will not use social media to contact children
- Should staff have any concerns about what they see or hear online, these will be brought to the attention of the Designated Teacher in line with the provisions of the school's Child Protection and Safeguarding Policy.

Google Classroom is accessible on a wide range of devices ranging from smart phones, tablets, laptops and PCs. However, the school recognizes the difficulties many parents have in being able to provide access to devices for all users in the home or in printing copies of the learning tasks they have downloaded. Therefore, the school will also supply paper copies of the learning tasks/answer sheets and these can be used in tandem with the activities which are uploaded to Google Classroom.

Video-conferencing, when used, will be via the C2K network to ensure security of the service. Video-conferencing will be appropriately supervised and parents will be required to give permission for their child to participate. Any video-conferencing undertaken will be part of agreed teaching and learning programmes agreed by the school.

The school will issue guidance to parents about supporting their children to stay safe online. In addition, the school will signpost parents to appropriate supporting resources available on www.thinkuknow.co.uk/parents and at www.ceop.police.uk/safety-centre

Publishing Pupils' Images and Work

St Joseph's Primary School's website –**www.stjosephscarryduff.com** will celebrate pupils' work and promote the school. As the school's website can be accessed by anyone on the Internet, the security of staff and pupils must be considered carefully. Editorial responsibility lies with the Principal and the UICT Coordinator to ensure that content is accurate and quality of presentation is maintained.

Written permission from parents/guardians will be obtained before photographs of pupils are published on the website. Parents will also give their permission for their child's image/work to be published on the website or social media outlets of outside agencies. The consent form is considered valid for the entire period that the child attends the school unless there is a change in the child's circumstances where consent could be an issue. Parents/ guardians may withdraw permission at any time by placing this request in writing to the Principal.

The point of contact on the website is the school address, info email account and telephone number. Home information or individual e-mail identities will not be published.

Full names will never be used alongside photographs anywhere on the website. Digital and video images of pupils are only taken with school equipment. Images are stored in a centralised area of the school network which is accessible only to school staff. Photographs of pupils are removed when they leave the school.

Further details available about the use of images is available from the Parental Consent slips

Authorising Internet Access

Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on responsible use. Pupil instruction in responsible and safe use should precede any internet access. All children must abide by the school's eSafety rules which will be displayed clearly in all rooms. Access to the Internet will be supervised.

Parents will be asked to give consent for their child to use the Internet in school within the constraints detailed in the school's eSafety policy. Parents will be asked to sign and return a permission form. Pupils must not use the Internet for unapproved purposes nor enter the folders or files of anyone else and they must adhere to the school's Rules for Responsible Internet Use.

The ICT Co-ordinator and Principal reserve the right to enter any pupil's account to ensure it is being used appropriately. Pupils must be aware that teachers have the right to enter any of the folders of the pupils in their class.

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. Pupils are not allowed to deliberately access files on the school network which belong to their peers, staff or others. Any such attempt will be treated as a breach of school rules with appropriate sanctions. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network and SIMS system.

Assessing the risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Staff, parents, governors and advisers will work to ensure that every reasonable measure is being taken.

Ensuring Internet access is safe

Pupils using the Internet will be appropriately supervised. Senior staff will conduct occasional checks to ensure that the filtering methods are effective in practice. If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to C2k by the Network Administrators /Principal.

Mobile Devices including Phones

Parents should be aware that mobile devices have downloadable capabilities (e.g. iPads, smart phones, Nintendo DS Lite, iPod touch or PSP) and children may be able to gain access to the internet through enabling mobile data on these devices. Therefore, if pupils have access to such devices Internet access becomes very difficult to regulate and photographs and video recordings can be taken of others without their consent.

Therefore, pupils are only permitted to carry mobile phones for use in emergency situations or for parents to check up on a child's safety either before/after school hours i.e. when on route to or from school or at post school childcare. Children should switch

off their phone on arrival at school and these may only be switched back on again when the pupil leaves the school premises. It should be noted that phones are brought into school at the owner's own risk.

If a pupil is found to be using a mobile phone on school premises without prior permission, the staff member who observes this will have authority to take the phone from the child. Parents and guardians can subsequently collect it from the school office.

Parents should ensure that all calls relating to a child must come through the school office and parents should not seek to contact their child directly on the child's mobile phone. Parents should note that school staff are not permitted to disclose the telephone numbers of any children to other children and/or parents.

Staff must ensure that their mobile phones are switched off during class contact time. Staff are not permitted to make or receive phone calls in the classroom. Emergency calls may be taken outside the classroom in the designated area i.e. the staffroom. Staff are not permitted to use their mobile phones to take photographs of children and they should not share their mobile numbers with parents or pupils. Staff should also be professional if sharing any personal business on social media sites.

Security of the school's internet access

Security of the school's internet access (including the Meru wifi network) is ensured through the C2K's filtered system.

Handling complaints regarding Internet use

Complaints of internet misuse by pupils will be dealt with by senior members of staff. As with drugs issues, there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies. Pupils and parents will be informed of the complaints procedures. Deliberate access to inappropriate materials by any user will result in the incident being logged in the eSafety incident log book.

Sanctions available for use with pupils include interview/counseling and, if appropriate, informing parents or carers. A pupil may have e-mails, Internet or computer access denied for a period of time depending on the nature of the incident.

Any complaint about staff misuse must be referred to the Principal. Complaints of a safeguarding nature must be dealt with in accordance with the school Child Protection Policy and procedures.

Communicating the Policy

Guidance on eSafety (SMART) and Rules for Responsible Internet Use will be displayed in all classrooms and the UICT Suite and will be discussed with pupils at the start of the year. Specific reference will be made by teachers at the beginning of every school year and at relevant points throughout the year e.g. Rules/Safeguarding Week/ Friendship Week/circle time/PDMU lessons. Pupils will be informed that network and Internet use will be monitored.

All staff including teachers, supply staff, classroom assistants and support staff will be provided with the Acceptable Use of the Internet Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and 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 outside of school.

Parents will be informed about the policy through its inclusion in the Pastoral Care Guide for Parents which is issued to each family and is displayed in the Parents' Information section of the school website.

Monitoring and Review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ELearning Co-ordinator. The effectiveness of the policy will be reviewed annually.

Addendum

- Network administrators reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibly. They will respect the right to privacy whenever possible.

- Any parent or member of staff who wishes to discuss this document can put any questions to:-

Mrs P Downard (Acting Principal)
or
Mr J Cherry (eLearning Co-ordinator)

This document is based on 'Acceptable Use of the Internet and Digital Technologies in Schools' (DE Circular 2007/1 – 18 June 2007) and 'eSafety Guidance' (DE Circular 2013/25)

St Joseph's Primary School

Acceptable Use of the Internet Statement

For Staff

.

- The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Acceptable Use 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 must sign a copy of this Acceptable Use of the Internet Statement
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems, is forbidden;
- Use of an iPad supplied by the school should be considered the same as any other technology tool provided by the school and thus staff must abide by the terms of the school's Acceptable Use Policy with regard to iPad use
- To ensure that all apps meet with the requirements of the school's eSafety and Acceptable Use policy the eLearning Co-ordinator will be responsible for authorizing the purchase of all apps installed on school devices
- Staff must inform the eLearning Co-ordinator of any apps that do not meet said requirements so that these can be removed from the device
- The eLearning Co-ordinator will only use an account in the name of the school and the school email address for all app purchases
- iPads should not be used to store personal documents such as video or audio material other than that which is directly related to school needs
- Apps that could be considered to be only for personal use or deemed not suitable for the classroom must not be installed on an iPad
- Use of the camera function on an iPad is only permitted in line with the whole school Child Protection Policy
- In the case of loss, theft or other damage of an iPad occurring outside school to co-operate fully with any investigation being conducted into the loss/theft/damage by any outside agency
- Ensure that pupils only use the iPad for curricular purposes under a controlled environment in the presence of a member of staff
- 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;
- Copyright of materials must be respected;
- All Internet activity should be appropriate to staff professional activity or the student's education. Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise school use;

- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded or may be sent inadvertently to the wrong person;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Users must access only those sites and materials relevant to their work in school. Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed.

Full name … … … … … … … …

Signed … … … … … … … … Date … … … … … … … … … … … … …

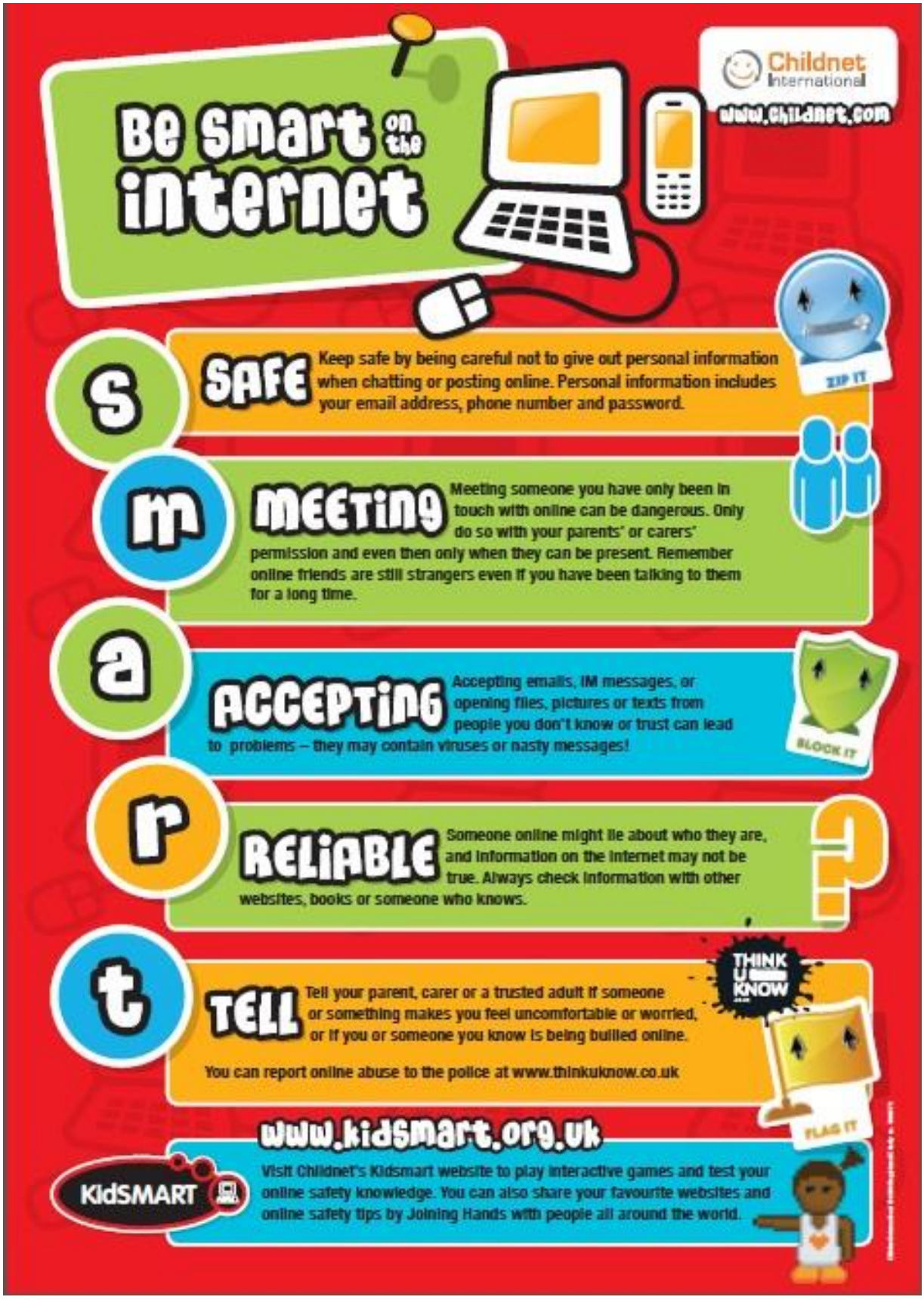
St Joseph's Primary School

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others**.**

- I will ask permission before entering any website unless my teacher has already approved this site. I will always quote the source of information gained from the internet in the documents I produce.
- On a network I will use only my own login and password which I will keep private.
- I will not look at, change or delete other people's files.
- I will not bring portable drives into school without permission.
- I will only e-mail people I know or my teacher has approved.
- The messages I send will be polite and responsible. I understand that the use of strong language, swearing or aggressive behavior is not allowed when using email.
- When sending e-mail, I will not give my home address or phone number or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I understand I am not allowed to enter Internet Chat Rooms when using school computers/ iPads
- If I see anything I am unhappy with or I receive messages I do not like I will tell teacher immediately.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules I could be stopped from using the Internet or computers and my parents may be informed

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.


Childnet International
www.childnet.com
Be Smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.
ZIP IT
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
BLOCK IT
r
RELIABLE
Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW
FLAG IT
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by joining Hands with people all around the world.

References

The following websites provide additional information for parents as well as some useful games/activities for children

www.thinkuknow.com

www.kidsmart.co.uk

www.getsafeonline.org

www.bbc.co.uk/chatguide

www.childnet.com

www.digizen.org

www.chatdanger.com

www.childnet.com/sorted

www.saferinternet.org.uk

APPENDIX 2

Dear Parents

Your child will have access to the Internet as part of his/her curriculum. Electronic information handling skills are a fundamental part of the preparation for citizenship and future employment. Developing the children's ICT skills is an important element of our work in St. Joseph's and that includes guided educational use of the Internet.

The school Internet access is provided through a filtered system that restricts access to inappropriate materials. The system is provided through Education Network (NI) and every endeavour is made to ensure that the restrictions in place limit the risk of children accessing inappropriate materials.

I would ask you to read the 'Rules for Responsible Internet Use' set out below and if you are in agreement I would be grateful if you would sign the consent form so that your child may continue to use Internet at school.

Please contact me should you wish to discuss any aspect of Internet use and may I thank you for your continuing support.

Yours sincerely

P. Downard

Mrs P Downard
Acting Principal

PARENTAL CONSENT FORM

Photographs and recordings of pupils for School, family and press are a source of pride to both the pupils and their families. Taking, keeping and publishing photographs and video footage involves processing personal data under data protection laws.

To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain express consent for the use of a pupil's image in school displays, performances, newsletters, prospectus and our website, virtual learning environment and school app.

In all instances below, the image or footage may be of an individual, small group, class or classes. Where pupils are named, we will use first names only unless we have sought prior permission from you to publish full names (***newspaper and media companies will often use a full name and we will not seek further permission for this**).

We will only use photographs and footage where pupils are appropriately dressed to reduce the risk of inappropriate use of the images or footage.

Please be aware that websites and social media can be viewed throughout the world and not just in the United Kingdom where UK law applies. Our current website is www.stjosephscarryduff.com

We may continue to use your child's image or footage after they have left the school in promotional materials or on our website

We will not include personal email, postal addresses, telephone or fax numbers on our website or in any printed materials

We may include a pupil's written work, projects and artwork including portraits of other pupils on our website and in promotional materials

This consent form is valid for the academic year September 2019 to June 2020. It will be updated on an annual basis. Consent will also be refreshed where any changes to circumstances occur.

Consent can be withdrawn at any time by notifying the Principal and completing a new copy of this form. If you do not consent to a particular use of your child's information, your child will not suffer any detrimental effect as a result.

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Principal. A new form will be supplied to you to amend your consent accordingly and provide a signature.

	I Agree	*I Disagree*
I permit my child's photographs, voice recordings or video image to be displayed within the school e.g. displays in reception, classrooms or corridors		
I permit my child's photograph to appear in any school publication and I understand that my child may be named in the caption or article associated with the image. I also understand that such publications may be used by the school for promotional purposes.		
I give permission for my child's photograph, voice recordings, video image or work to be used on the school website/virtual learning environment and school app.		
My child may be named in the associated captions or articles on the website/virtual learning environment and school app. In order to ensure individual children cannot be identified, full names will not be used.		
I give permission for my child's photograph, voice recordings, video image or work to be displayed on the school website and social media platforms of our Shared Education partner schools.		
I permit my child to take part in video conferencing with other schools/partner organisations and webinars hosted by partner organisations.		
I permit my child's photograph to be published in any newspaper/parish magazine/local magazine and I understand that my child may be named in the caption or article associated with the image.		
I permit my child to participate in school events which may be photographed or videoed by other parents or professionals acting on behalf of the school.		
I give permission for visiting media organisations to take photographs or video footage of my child and use them in local or national publications, on websites and on radio and television programmes		
I permit my child to feature in footage recorded for the purposes of teacher training which is shared with other teachers in the school and externally e.g. by Dept. of Education and/or Education Authority for use in their productions.		
I give permission for my child's image/work to appear on the website or social media platforms of other organisations e.g. Universities, charities and other agencies who work with the school		
I give permission for my child to access the internet, including email. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials and that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.		
I have read and accept on behalf of my child the school's Rules for Responsible Internet Use (see eSafety and Acceptable Use of Digital Technology Policy which is displayed on the Policies section of the school website and app).		
I permit my child to leave the school premises for school trips, or visits to the Church, Parish Hall or Carryduff GAC's football pitch.		
I consent to receiving marketing material via email and/or printed copy from St Joseph's PFA		
I consent to receiving marketing material via email and/or printed copy from the school's partner organisations e.g. Parish of Drumbo and Carryduff, Carryduff GAC, Carryduff Colts, Lisburn and Castlereagh City Council, 1,2,3, After School Club, the school's After School Activities coaches/tutors		

Parent/Guardian _____