# Boscastle and Port Isaac

# Community Primary Schools

# E – Safety Policy

This policy must be read in conjunction with the Preventing Radicalisation and Extremism policy and all other policies relating to the safeguarding of children.

Spring 2017

Review 2019



Appendix

## 1. Introduction

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## 2. Context and Background

### The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

### Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:
• An effective range of technological tools
• Policies and procedures, with clear roles and responsibilities
• E-Safety teaching is embedded into the school curriculum and schemes of work

## 3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

**Head teacher**
The Head teacher ensures that the Policy is implemented across the school via the usual school monitoring procedures

**E-Safety Co-ordinator**
Our schools E-Safety Co-ordinator is the Head teacher. The head teacher is responsible for keeping up to date on all e-Safety issues and ensuring that staff are updated as necessary.

**Governors**
The School Governing body is responsible for overseeing and reviewing all school policies, including the E-Safety Policy.

**School Staff**
All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed. They should sign the Staff Acceptable Internet Use agreement annually. Class teachers should ensure that pupils are aware of the e-Safety rules, introducing them at the
beginning of each new school year.

**Pupils**
Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school.
They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school

**Parents**
Parents are given information about the school's e-safety and the parents' e-safety policy via the web site or as a hardcopy if requested. They are given copies of the pupil acceptable use agreement for information, and asked to support these rules with their children.

## 4. Technical and Hardware Guidance

**School Internet provision**
The school use the South West Grid for Learning (SWGfL) as our Internet Service Provider.

**Content Filter**
SWGfL use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and

generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Our ICT support is provided by TME.

• *All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.*
• *Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.*

**Downloading files and applications**
The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

• *Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.*

**Portable storage media**
• *Staff are not routinely allowed to use their own portable media storage (USB Keys etc). Permission should be sought from the e-Safety coordinator if portable media storage is to be used. If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT support company. (TME)*

**Security and virus protection**
The school subscribes to Sophos Antivirus software. The software is monitored and updated regularly by TME.

• *Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to TME.*

## 5. e-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

### Internet access at school

**Use of the Internet by pupils**
Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

**Access for all pupils**
In line with our inclusion policies across the school, we want to ensure that all out pupils have access to the Internet, particularly where this will directly support their learning.

**Out of Hours Provision**
There is an after-school homework club that runs weekly.
There will be no unsupervised access to the Internet at any time during out of hours provision.

**Using the Internet for learning**
The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. Using the Internet for learning is now a part of the Computing Curriculum. We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- *Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.*
- *Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.*
- *They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.*
- *They are taught how to carry out simple checks for bias and misinformation*
- *They are taught that web-based resources have similar **copyright status** as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.*

**Teaching safe use of the Internet and ICT**
We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, And we use the Kidsmart safety code to support our teaching in this area. Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES http://www.kidsmart.org.uk

The main aspects of this approach include the following five SMART tips:

- **S**afe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- **M**eeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- **A**ccepting 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**emember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- **T**ell your parent or carer if someone or something makes you feel uncomfortable or worried.

**Suitable material**
We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the

curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

**Non-Education materials**
We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.

**Unsuitable material**
Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:
1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator
3. Logging the incident – ICT Incident Log Book in the school office
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future

**Using E-Mail at school**
E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

• *We teach the use of e-mail as part of our ICT curriculum, and use appropriate pupil email accounts where necessary*
• *Pupils are not allowed to access personal e-mail using school Internet facilities*

**Chat, discussion and social networking sites**
These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas. Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.
We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

All commercial Instant Messaging and Social Networking sites are filtered as part of the LA

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

## Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use

in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

• *Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office or in the bags for pupils who may need them on their journey to and from school.*

**Cyberbullying - Online bullying and harassment**
Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

• *No access to public chat-rooms, Instant Messaging services and bulletin boards.*
• *Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.*

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

• *Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.*
• *Complaints related to child protection are dealt with in accordance with school child protection procedures.*

## Contact details and privacy
As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

**School and pupil websites – pictures and pupil input**
As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources. Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images

restricted.

**Deliberate misuse of the Internet facilities**

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom and pupils should be reminded of them regularly.
Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

**Sanctions will include:**

**Unsuitable material** (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Removal of Out of School Hours access to Internet
- Report to head teacher
- Meeting with parent/carer

**Offensive material** (e.g. pornographic images, racist, sexist or hate website or images etc)

- Incident logged and reported to Head teacher
- Meeting with parent/carer
- Removal of Internet privileges/username etc
- Removal of Out of School Hours access to Internet

Before allowing use of the internet again:

- Meeting with pupil and Parent/Carer to re-sign Internet use agreement
- Subsequent incidents will be treated very seriously by the head teacher, and may result in exclusion and/or police involvement.

**How will complaints regarding e-Safety be handled?**

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Given the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- All incidents will be recorded.
- Interview/counselling by class teacher, e-Safety Coordinator or head teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period.
- Referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about

staff misuse is referred to the Head teacher.

## 6. Use of the Internet and ICT resources by school staff

### The Internet

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.
We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

### Internet Availability

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use.

### ICT Equipment and Resources

The school also offers staff access to appropriate ICT equipment and resources which may include computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.
Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this e-Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used e.g. teachers using laptops or tablets at home as it remains the property of Boscastle and Port Isaac Primary Schools at all times.

### Professional use

Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home. Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the head teacher.

### E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address which must be used for all professional communication with colleagues, organisations, companies and other groups.
Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.
E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

**Online discussion groups, bulletin boards and forums, online chat and messaging**
We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.
The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

**Personal use of the ICT resources**
Staff may only use the schools' digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body. Teachers may take their work laptops and tablets out of school for professional purposes only e.g. preparation and planning of work. Staff must be aware of and abide by the schools' e safety policy which is outlined in the staff agreement form.

**Personal use of the Schools' Internet**

- *Teachers laptops may be used to access private e-mail accounts during lunchtimes and break times, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.*

**Use of mobile phones/SMART phones on the School's Premises.**
The school understand that staff may wish to use their phones for personal reasons at break times and lunchtimes. Phones should be switched off during lessons and stored safely in the staff room or in secure bags/briefcases

- *Staff may use phones during lunchtimes and break times in accordance with the staff agreement form and the social media policy.*

**Social Networking**
The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in the Social Media Policy.

Staff should adhere to the following principles:

***BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL***

- **Be conscious at all times of the need to keep your personal and professional lives separate. Do not put yourself in a position where there is a conflict between your work for the school or Local Authority and your personal interests.**

- Staff must not engage in activities involving social media which might bring Boscastle and Port Isaac Primary Schools or the Local Authority into disrepute.

- Staff must not represent their personal views as those of Boscastle and Port Isaac Primary Schools or the Local Authority on any social medium.

- Staff must not discuss personal information about pupils, Boscastle and Port Isaac Primary Schools or Local Authority staff and other professionals you interact with as part of your job on social media.

- Staff must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, Boscastle and Port Isaac Primary Schools or the Local Authority.

- Staff must be accurate, fair and transparent when creating or altering online sources of information on behalf of Boscastle and Port Isaac Primary Schools or the Local Authority.

**Copyright**
Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

## 7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- *When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.*
- *In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.*
- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*

- *Pupils must not take, use, share, publish or distribute images of others without their permission.*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website*

## 8. Data Protection Policy

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.
Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

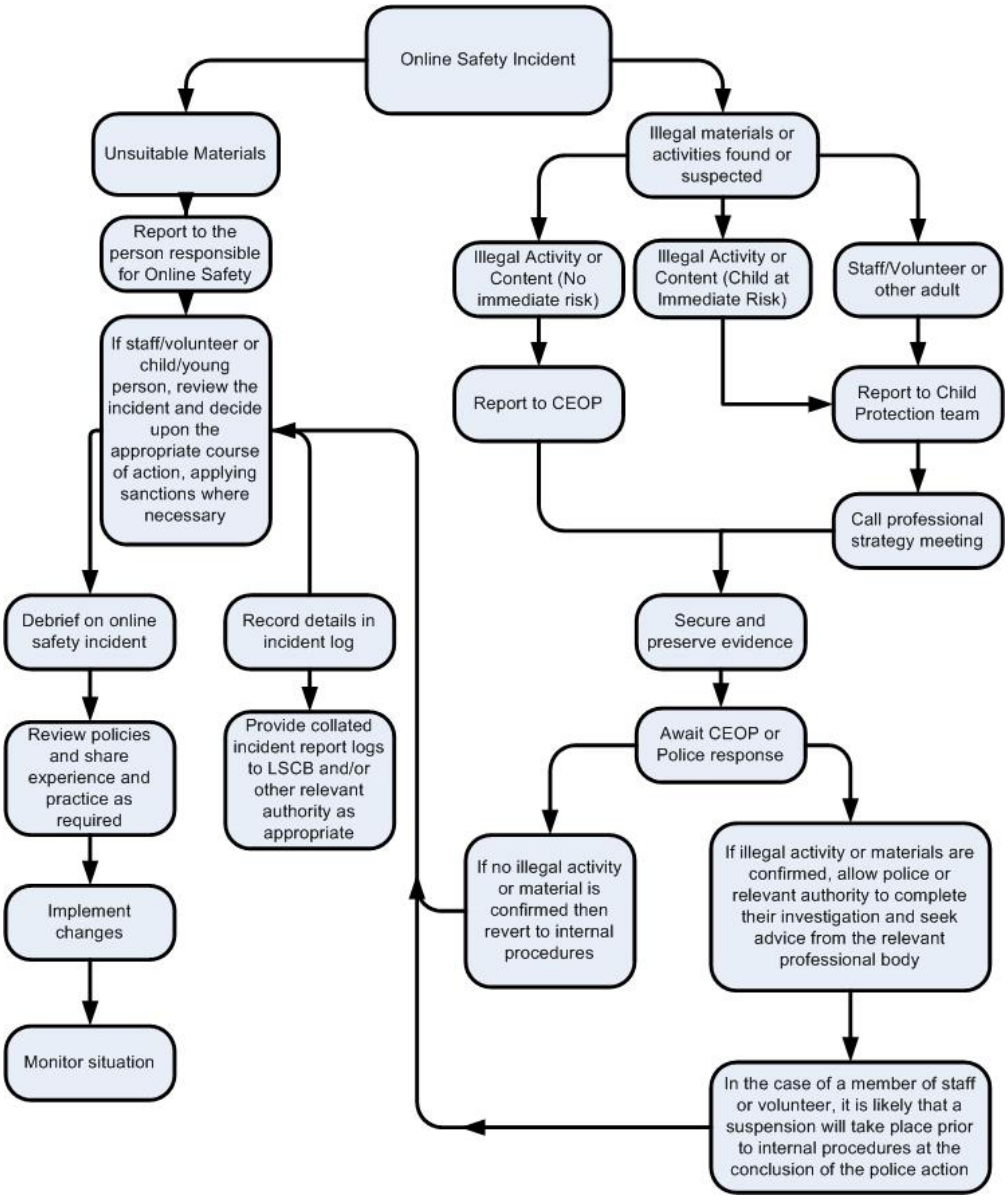
## 9. Responding to Incidents of Misuse of Online Services

### Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

### Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.




**Other Incidents**

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- *Internal response or discipline procedures*
- *Involvement by Local Authority or national / local organisation (as relevant).*
- *Police involvement and/or action*

**If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

- *Incidents of 'grooming behaviour'*
- *The sending of obscene materials to a child*
- *Adult material which potentially breaches the Obscene Publications Act*
- *Criminally racist material*
- *Other criminal conduct, activity or materials*
- ***Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.***

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## Boscastle and Port Isaac School Pupil Acceptable Use Policy Agreement Key Stage 1

**This is how we stay safe when we use computers:**

- I will ask an adult if I want to use the computer
- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

| | | |
|---|---|---|
| My name: | | Date |
| R - Signed (child): | | |
| Y1 - Signed (child): | | |
| Y2- Signed (child): | | |

# Boscastle and Port Isaac School Pupil Acceptable Use Policy Agreement Key Stage 2

I understand that I must use technology in a responsible way.

**For my own personal safety:**

- I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.
- I understand that my use of the internet will be monitored
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

**For the safety of others:**

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

**For the safety of the school:**

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal ICT kit if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

| Name: | | Date |
|---|---|---|
| Y3: Signed | | |
| Y4: Signed | | |
| Y5: Signed | | |

| | | |
|---|---|---|
| Y6: Signed | | |

Be Safe

Tell an Adult

Don't talk to someone
That you don't know

# SMART

**S**afe

**M**eeting

**A**cceptable

**R**eliable

**T**ell


Keep personal information **Safe**. **Meeting someone you don't know** is dangerous. Do not

accept emails or messages from people you do not know. Not all websites are reliable. Tell a responsible adult if you feel worried.

## Boscastle and Port Isaac

### e-Safety Policy Staff, Governors and Volunteers Agreement Form

This document covers use of school digital technologies, networks etc both in school and out of school.

**Access**

- I will obtain the appropriate log on details and passwords from the ICT Co-ordinator.
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access school ICT systems or resources

**Appropriate Use**

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-Safety coordinator or member of the SMT.

**Professional Conduct**

- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

**Personal Use**

- I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
- I understand that I may access private e-mail accounts during the availability periods outlined

above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or social networking sites

**Email**
- I will only use the approved, secure email system for any school business
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

**Use of School equipment out of school**
- I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will return school equipment regularly (to be agreed with ICT Administrator) to be checked and updated
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software

**Teaching and Learning**
- I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet
- I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in My classroom practice
- I will only use the Internet for professional purposes when pupils are present in an ICT suite, or a Classroom with Internet access

**Photographs and Video**
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
- I will never associate pupil names or personal information with images or videos published in School publications or on the Internet (in accordance with school policy and parental guidance)

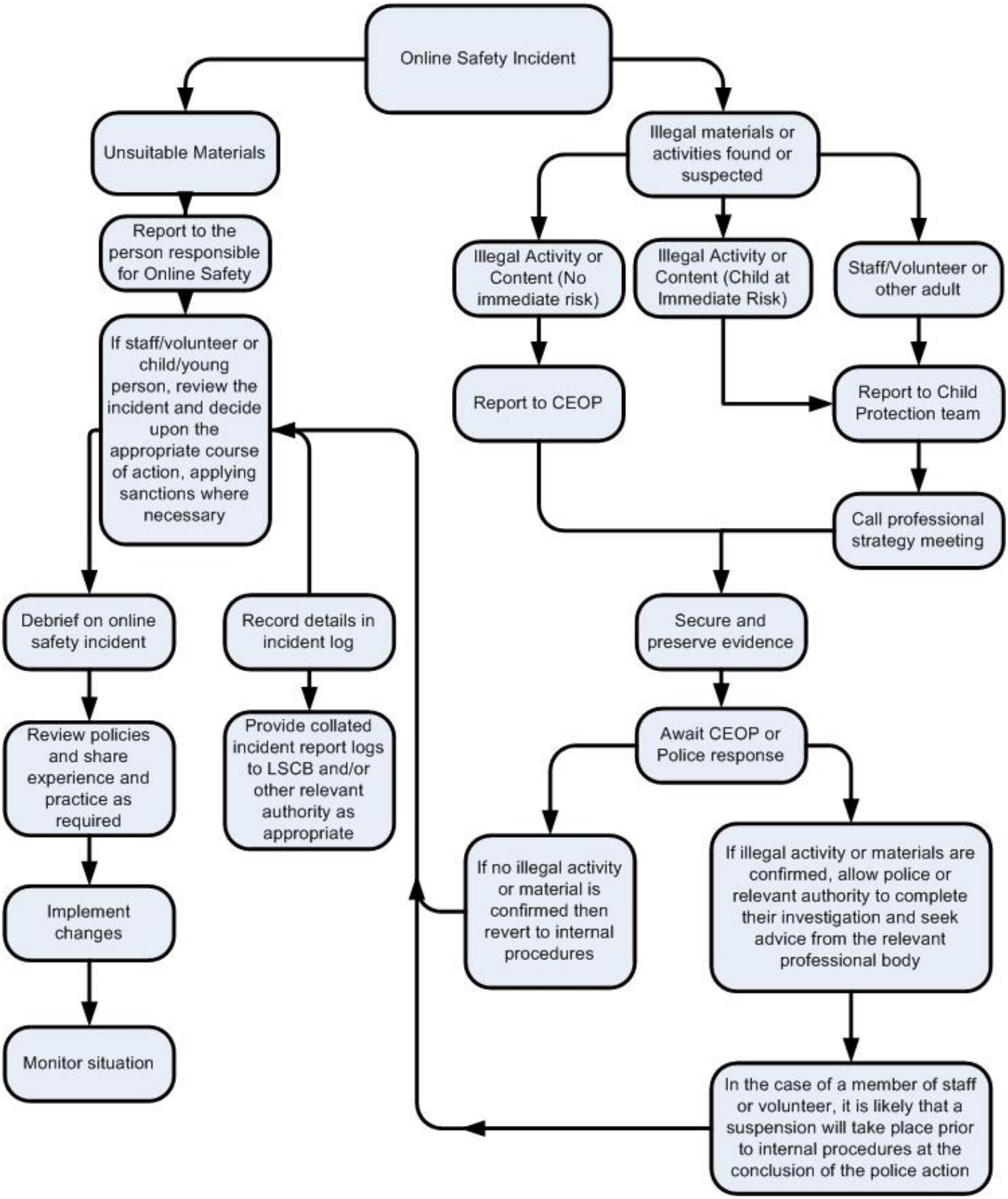
**Data protection**
- I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
- I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media
- I will ensure that I follow school data security protocols when using any confidential data at any Location other than school premises
- I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission
- I understand that data protection policy requires that any information seen by me with regard to

staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

**Copyright**

- I will not publish or distribute work that is protected by copyright
- I will encourage pupils to reference online resources and websites when they use them in a report or publication.

Signed ……. Date …….


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

**Federation of Boscastle C.P. & Port Isaac C.P. Schools**

**E-safety Policy for Parents**

**Reviewed Spring 2017**

**Next Review Spring 2019**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

This provides a summarised version of the school's e-safety policy which is available in its entirety on our website or from the office.

## Teaching and support staff

Teachers and support staff will be instrumental in ensuring that children are supported in developing their understanding of digital citizenship, acceptable use and e-safety.

All staff will be required to sign and abide by the staff and volunteer acceptable use policy which clearly defines what is and is not permissible when utilising school systems and equipment. Further they are bound by rules of professional conduct aimed at protecting children and their own professional integrity.

The policy ensures that all staff and volunteers including parent teacher association members will be responsible users and stay safe while using information technologies for educational, personal and recreational use.

## Pupils

Pupils are responsible for using the school ICT systems in accordance with the Pupil acceptable use policy which they will be expected to sign. The policy was formulated in collaboration with children and encompasses the SMART Rules:

**S**afe- I will not give out personal information about myself

**M**eeting- I will not arrange to meet with people I have only met online

**A**ccepting- I will not accept emails, instant messages, pictures, files or texts from people I don't know and trust

**R**eliable- I understand that not all information I receive via the internet is true or accurate

**T**ell- I will tell a parent or trusted adult if someone or something makes me feel uncomfortable or worried.

In addition the policy stipulates that children should behave, in accordance with the principles of good citizenship, responsibly and with the same good conduct online, as would be expected offline.

**Technical –infrastructure/equipment, filtering and monitoring**

The schools ICT systems are managed in ways that ensures the school meets e-safety requirements. Systems are in place to filter and monitor activity on line including reporting incidents. All users have clearly defined access rights to school ICT systems. There will be regular reviews and audits of the safety and security of the school ICT systems.

**Responding the incidents of misuse**

There may be times when infringements of the policy could take place, through careless, irresponsible or, deliberate misuse. There are a range of responses that will be made to any apparent or actual incidents or misuse. However, any illegal activity which involves child abuse, breaches of the Obscene Publication Act, criminally racist material or other criminal conduct, activity or material will be reported to the police.

**Parents and Carers**

E-Safety however, is not only a school issue. Parents must play an integral part in educating children about using communication technologies responsibly and safely. The messages need reinforcing. One of the ways in which this can be modelled is by ensuring that all communicating with school is through the formal channels i.e. school email, by phone or in person. It is not appropriate for parents to contact teachers through their personal phone (mobile or landline), by social media site or to request that teachers become friends on social media sites.

Finally we understand that parents want to take pictures of their children at the various events and activities that take place in school. All parents have given permission for the school to take photographs of the children for use by the school. However, this permission does not include parents' rights to photograph other children. Following the recent guidance from the Information Commissioner, the local authority advice regarding parents taking photographs in school states family photographs for personal use **only** are permitted. Where individuals want to use a photo in the press, on a website or magazine then child's parent/carer's permission or schools permission is required. This would obviously include posting any photographs on any social networking site such as "Facebook" Therefore, as a condition of taking photos and other images, parents need to ensure they do not upload the images of children who are not their own.

Signed

Date