**Steyning CE Primary School, Steyning**

**Online Safety Policy**

***Creating a Brighter Future***

## 1. Introduction

This policy defines requirements for managing online safety in all aspects of Steyning Primary School both on and off the premises. The policy was first written in the Spring Term 2014 and agreed by the Senior Leadership Team (SLT), online safety Team, staff and Governors.

The school will have nominated online safety representatives for both staff and Governors. Their responsibility is to ensure the implementation and maintenance of this policy.

The policy and its implementation will be reviewed and updated annually by the online safety Team and the Governing body.

## 2. Teaching and Learning

*The future of our children will depend on their understanding and use of the internet.*

Internet use is part of the statutory curriculum and is a necessary tool for learning.
The Internet is a part of everyday life for education, business and social interaction.

An annual survey of each class will be carried out to establish what specific areas of the internet and safety are applicable to those particular children, in order to inform the teaching programme.

Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be taught never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging (IM) and email addresses, full names of friends/family, specific interests and clubs, etc.

Pupils will be taught about security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
Pupils will use age-appropriate tools to research Internet content.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

## 3. Acceptable Use - Within School

Networked resources, including Internet access, are potentially available to all pupils and staff in the school as well as regular helpers. All users are required to follow the conditions laid down in the signed agreement form for adults and pupils. See Appendix 1 and 2.

Any breach of these conditions may lead to withdrawal of the user's access and in some circumstances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the Internet or the school's Intranet is not allowed. All computer systems will be regularly monitored to ensure that they are being used responsibly.

All websites used within school or recommended for use outside of school will be checked prior to use to ensure suitability.

### 3.1 Personal responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Adults and pupils will be expected to use the resources for the purpose for which they are made available. Users will accept personal responsibility for reporting any misuse of the network to the schools online safety representative or Head Teacher.

Users are expected to utilise the network in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but guidelines are given in the agreement forms (Appendix 1 and 2) which must be signed by adults and pupils.

## 4. School Management Information Systems

### 4.1 Local Area Network LAN

Servers will be located securely and physical access restricted.

The server operating system must be secured and kept up to date.

Virus protection for the whole network must be installed and current.

Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Passwords for the children are unique, and randomly generated through DB Primary.

Passwords should never be shared with anyone else.

Passwords should not be written down in view of other people.

The use of user logins and passwords to access the school network will be enforced.

**4.2 email**

Children's internet based communication within school will be through their DB Primary accounts, which are only usable internally. Any external communication will be through DB Primary's 'SafeMail' system which is controlled by the teachers.

Pupils and parents/carers will only use official school provided email accounts to communicate with staff.

Children's access in school to external personal email accounts will be blocked.

**4.3 School Website and Virtual Learning Environment (VLE)**

The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

Team Leaders will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

The school website will comply with intellectual property rights, privacy policies and copyright.

Staff will routinely monitor the usage of the VLE by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

Pupils/staff will be advised about acceptable conduct and use when using the VLE.

Areas of VLE used by children for their school work will only be accessible by pupils and teachers. Parents/carers can view the VLE with limited/relevant access.

All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
When staff, pupils, etc. leave the school their account will be disabled.

Any concerns about content of the VLE will be referred to the staff online safety representative.

A visitor may be invited onto the VLE by the VLE administrator; in this case, there may be an agreed focus or a limited time slot.

**4.5 Use of Digital Images/Video**

Use of ***personal*** cameras/phones/tablets by staff within school is not permitted.

Written permission from parents or carers will be obtained before photographs of pupils are published.

When a parent does not agree to their child's photograph being used, the Head Teacher/online safety representative must inform staff, and staff must make every effort to comply.

Any images of a young person, who is under a court order, will not be recorded and published without explicit consent.

Pupil's names will not be displayed with images. This includes photographs, videos, TV presentations, web pages and the press, etc. Where named images must be used then specific written permission from Parent's or Guardian's must be obtained in order to comply with the Data Protection Act 1998.

The recording of images of children participating in extra-curricular events that are taken for personal use are exempt from the Data Protection Act. These include uses such as parents taking photographs of Sports Day or a grandfather videoing a school nativity.

Staff will monitor the use of cameras and anyone behaving inappropriately at extracurricular events. If there are concerns, the Head Teacher can require the person to cease using the camera or leave the premises.

All children featured will be appropriately dressed with outer clothing garments covering their torso from at least the bottom of their neck to their thighs, (i.e. a minimum of vest/shirt and shorts).

The photograph should ideally focus on the activity and where possible images will be recorded in small groups.

The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**4.6 Social Networking, Social Media and Personal Publishing (in school)**

The school will control access to social media and social networking sites.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.

Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

If used, personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils underage use of sites.

**4.7 Filtering**

The school's broadband access is automatically filtered by the schools ISP. The school has the ability to unblock particular sites as agreed by the Head Teacher.

If staff or pupils discover unsuitable sites, the URL will be reported to the online safety representative who will then record the incident and escalate the concern as appropriate.

Any material that the school believes is illegal will be reported to the Police.

**4.8 Other Internet Based Applications e.g. forums, video conferencing etc.**

Any devices or applications outside of normal network use will be discussed and approved by the online safety representative prior to any use. All risks against benefits will be assessed and if considered necessary the Head Teacher's approval will be sought.

**4.9 Data Protection**

All Personal Data held will be held in accordance with the Data Protection Act 1998 and should be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Any information stored on removable media (USB sticks, etc.) should be encrypted.

**4.10 Services**

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or human errors / omissions. Use of any information obtained via the network is at the user's risk.

**4.11 Network Security**

Users are expected to inform the network administrator or the Head Teacher immediately a security problem is identified. Users will not demonstrate problems to other users. Users will login with their own user ID and password, where applicable, and will not share this information with others. Users identified as a security risk will be denied access to the network.

**4.12 Physical Security**

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras will be securely locked away during school holidays and open school events, e.g. Christmas Fair.

Digital cameras and other portable ICT equipment will be placed in a secured cupboard when not in use and switched off at the end of each day. Staff should ensure that classroom blinds are lowered at the end of each day. Portable ICT equipment should be security coded.

### 4.13 Wilful Damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses; the use of software from unauthorised sources is prohibited. Any software to be installed on the school network will be authorised by the Subject Leader and Network Administrator.

## 5. Risk and Incident Management

### 5.1 Risk

The school will take all reasonable 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. Neither the school nor WSCC can accept liability for the material accessed, or any consequences resulting from Internet use.

### 5.2 Incidents

All members of the school community will be informed about the process for reporting online safety concerns, such as breaches of filtering, cyber bullying, illegal content, etc.

The online safety representative will record all reported incidents and actions taken in the School online safety incident log and/or the Class Behaviour Log.

The designated Child Protection Officer will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.

The school will manage online safety incidents in accordance with the school discipline/ behaviour policy where appropriate.

The school will inform parents/carers of any incidents or concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team and the Police.

If the school is unsure how to proceed with any incidents or concern, then the incident may be escalated to the Area Children's Officer or the County online safety Officer.

Any incidents regarding staff misuse will be reported to the Head Teacher.

### 5.3 Cyber bullying

At Steyning Primary School we define cyber bullying as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone".

Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.

There are clear procedures in place to support anyone in the school community affected by any type of bullying.

All incidents of cyber bullying reported to the school will be recorded.

There will be clear procedures in place to investigate incidents or allegations of cyber bullying.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

## 6. Personal Devices

### 6.1 Mobile Phones and Other Connected Devices

Children are not permitted to use mobile phones or other connected devices (internet enabled) within school.

Mobile phones carried by staff during teaching hours will be muted to silent or switched off and will not be used.

Staff are free to use mobile phones in school outside of teaching hours.

The sending of abusive or inappropriate messages or other content to staff or pupils is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the school setting in a professional capacity. An exception will be when staff need to contact families during school residential trips or visits.

If members of staff have a reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

Staff will not use mobile phones to take photos or videos of pupils and will only use work-provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action may be taken.

### 6.2 Social Networking, Social Media and Personal Publishing (outside school)

All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.

The sending of abusive or inappropriate messages or other content to staff or pupils via personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

Access by pupils to staff social networking accounts is forbidden.

Staff will be mindful of content and material published from their accounts in terms of its distribution to ensure that the school and its staff, pupils and WSCC and the associated community is in no way compromised in terms of confidentiality and personal well-being.

Staff are expected to conduct their online activities in a way that represents their professional standing.

Passwords used for online accounts are recommended to be at least six characters long including numbers and capitals. They should not be shared with anyone else or written down so that others can see them.

Written by: Online safety Working Group - February 2014

| | |
|---|---|
| Policy Adopted: | May 2014 |
| Policy Reviewed: | - |
| Review requirement: | Every 3 years |
| Date for next review: | May 2017 |

Appendix 1 Staff Acceptable Use Agreement
Appendix 2 Pupil Acceptable Use Agreement