Steyning CE Primary School, Steyning

Online Safety Policy

Policy Adopted:	February 2018
Policy Reviewed:	January 2022
Review requirement:	Annually
Date for next review:	January 2023

1. Introduction

This policy defines requirements for managing online safety in all aspects of Steyning Primary School and applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital technology systems, both on and off the premises.

Schedule for Monitoring

This online safety policy was approved by the Governing Body on:	*27 January 2022*
The implementation of this online safety policy will be monitored by the:	*Online Safety Team and Senior Leadership Team*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*January 2023*
Should serious online safety incidents take place, the following external agencies should be informed:	*LA Safeguarding Officer, Academy Group Officials, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Questionnaires of
    - pupils
    - parents/carers
    - staff

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. Pupils use the Internet widely outside school and need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The purpose of Internet use in school is to prepare pupils for the opportunities and challenges they will face in their future, to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

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. All computer systems will be regularly monitored to ensure that they are being used responsibly.

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.

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor/Director will include:

- regular meetings with the Online Safety Coordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.

The Headteacher and Senior Leaders should:

- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Be responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement
- they report any suspected misuse or problem to the Headteacher/Online Safety Lead for investigation/action/sanction
- all digital communications with pupils/parents and carers should be on a professional level and only carried out using official school systems

Pupils are responsible for:

- using the school digital technology systems in accordance with the pupil acceptable use agreement

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

4. School Management Information Systems

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

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.

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 Cloud technology

The cloud describes systems or services that are hosted and managed online, rather than locally in the school building. Computers, including mobile devices and smartphones, now increasingly operate in this way.

When using cloud systems, the school considers the following as good practice:

- Staff should be trained in how to use the cloud for storage and work purposes.
- The user of the cloud deletes all copies of personal data within a timescale that is in line with the schools deletion schedule.
- Only members of the school with a school email account should have access to the cloud technology.
- There should be a system in place to create, update, suspend and delete user accounts, to remove access from employees when they leave the organisation or to reset forgotten, lost or stolen credentials.
- Confidential information should not be shared on the cloud with anyone outside of the organisation.

4.3 Email

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers must be professional in tone and content
- Students will be provided with individual school email (Gmail) addresses for educational use.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- Any external communication will be to authorised recipients, who will be placed on a 'white-list' which is controlled by an administrator.
- Children's access in school to external personal email accounts will be blocked.

4.4 School Website

The contact details on the website will be the school address, email and telephone number.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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.

When staff, pupils, etc. leave the school their account will be disabled.

4.5 Use of Digital Images/Video

- 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.
- 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.
- 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/academy 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 students/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' full names will not be displayed, particularly in association with photographs. Where named images must be used then specific written permission from Parent's or Guardian's must be obtained.
- 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.
- 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.
- 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

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

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.

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.

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.

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts
- A code of behaviour for users of the accounts, including
  - Systems for reporting and dealing with abuse and misuse
  - Understanding of how incidents may be dealt with under school disciplinary procedures

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

4.7 Filtering

Internet access is filtered for all users. Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. The school's broadband access is automatically filtered by the school's 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/GDPR – General Data Protection Regulations

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded

- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school/academy personal data to personal devices except as in line with school policy
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

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. All users will be provided with a username and secure password. Users are responsible for the security of their username and password. Users will login with their own user ID and password. 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, iPads 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

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. It is vital that 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.

In the event of suspicion, these steps should be followed:

- Staff will record all reported incidents and actions taken onto Child Protection Online Management System (CPOMs) using the 'online safety' category.
- The designated safeguarding leads 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.
- 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.

- 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
  promotion of terrorism or extremism
  offences under the Computer Misuse Act (see User Actions chart above)
  other criminal conduct, activity or materials
- 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 Social Care team at the local authority and / or the Police.
- Any incidents regarding staff misuse will be reported to the Head Teacher or in their absence the designated safeguarding lead.

5.3 Online bullying

At Steyning Primary School we define online bullying as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone". Online 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 online bullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of online 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 any member of staff is contacted by a parent in regards to a school issue, which may ask for information regarding their child or another, they should reply with the following text: Dear xxxx, I am afraid that school policy forbids me from discussing this with you. Please contact the school directly and I am sure that they will be able to assist. Thank you.
- 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.

Appendix 1

Staff Acceptable Use Agreement

School networked resources, including the Internet and email, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in this agreement. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

The Computing Subject Leader deals with curriculum and learning issues (currently Ruth Dillingham).
Software problems should be reported to Lucie Martin, hardware problems reported to our on site premises manager, Adrian Emery, and emergencies or complex issues will be directed to our external support company (Technology and Solutions).

CONDITIONS OF USE

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Computing subject Leader.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos/code of conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to children.
6	I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
7	I will ensure that all my login credentials (including passwords) are unique to the school and not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately. If I think my email has been hacked, I will report it to Technology Solutions to be resolved and inform the Headteacher.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under another user's username I will **not** continuing using the machine – I will log it off immediately.
11	I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital video/images. I will not use my personal equipment to record these images, unless I have permission to do so.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not allow unauthorised people access to my email, internet or school network
14	I will not use the network in any way that would disrupt use of the network by others.
15	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to a member of the SLT
16	I will not use 'USB drives', portable hard-drives or personal laptops on the network or for storing and school related information.

17	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
18	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
19	I will only use social networking sites in school in accordance with the school's policies.
20	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 in any way.
21	I will support and promote children being safe and responsible in their use of the Internet and related technologies.
22	I will not send or publish material that violates GDPR requirements or breaches the security this act requires for personal data, including data held on the SIMS Learning Gateway.
23	I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
24	I will not harm or destroy any equipment or data of another user or network connected to the school system.
25	I will ensure that portable computer equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
26	I will ensure that any sensitive data that is sent over the Internet will be appropriately secured.
27	I will embed the school's Online safety curriculum/policy into my teaching
28	I understand that it is not appropriate to use mobile phones in the classroom during lesson time, unless in the case of emergencies, when permission will have been given by a member of the school leadership team. (Incoming emergency phone calls should be directed through the school office)

Additional guidelines

- Staff must comply with the Acceptable Use policy of any other networks that they access.

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 your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the school secretary, Lucie Martin, immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of children are published. Also, examples of children's work must only be published (e.g. photographs, videos, TV presentations, web pages, etc.) if written parental consent has been given.

✂ -

Staff User Agreement Form

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

I will use the network in a responsible way and observe all the restrictions explained in this agreement.

I agree to report any misuse of the network to a member of the SLT.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to a member of the SLT.

Lastly, I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the school secretary, Lucie Martin.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: ____

Signature: ______________________________

Date: _ _ /_ _ /_ _ _ _

Appendix 2

Online-Safety Pupil Acceptable Use Agreement

All children must follow the rules when using school computers.

Children that do not follow these rules may find:

- They are not allowed to use the computers
- They can only use the computers if they are more closely watched.

Computer Rules	
1	I will only use the computers in school for school purposes
2	I will only use polite language when using the computers.
3	I must not write anything that might upset someone or give the school a bad name.
4	I know that my teacher will regularly check what I have done on the school computers.
5	I know that if my teacher thinks I may have been breaking the rules, they will check on how I have used the computers in the past and my parents will be contacted if the school is worried about my online safety.
6	I must not tell anyone my name, where I live, or my telephone number - over the Internet. I will not arrange to meet anyone unless this is part of a school project approved by my teacher and a responsible adult comes with me
7	I will keep my password secret and only tell my parents.
8	I must never use other people's usernames and passwords or computers left logged on by them.
9	If I think someone has learned my password then I will tell my teacher.
10	I will always log off after I have finished with my computer.
11	I know that e-mail is not guaranteed to be private.
12	I will only open email attachments from people I know or who my teacher has approved.

13	I will not use the computers in any way that stops other people using them.
14	I will report any websites that make me feel uncomfortable to my teacher.
15	I will tell my teacher straight away if I am sent any messages that make me feel uncomfortable.
16	I will treat all computer equipment carefully and respectfully
17	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.
18	I will be responsible for my behaviour when using computers because I know that these rules are here to keep me safe.

Student User Agreement Form

I agree to follow the school rules when using the school computers. I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the computers sensibly to my teacher.

I know that I do not have to accept anyone being unkind or bullying me when I am online and I agree to tell my teacher or another member of staff about anything that makes me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Student Name: ____

I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers may have their use stopped, more closely monitored or past use investigated.

Parent/Carer's/Guardian's Name: ____

Parent/Carer's/Guardian's Signature: _________________________________

Date: __/__ /_____

Appendix 3

School IT Device Loan Agreement.

Part of Steyning CofE Primary School's Improvement Plan is to provide school IT devices to some staff to assist in the delivery of the Curriculum. The Head Teacher has agreed that devices will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time

As a member of staff to whom a device has been loaned I have read and agree to the following terms and conditions that apply while the laptop is in my possession:

1 The devices and any accessories provided with it remain the property of Steyning Primary School and is strictly for my sole use in assisting in the delivery of the Curriculum or school administration.

2. I understand insurance cover for WS maintained schools provides protection from the standard risks but excludes theft from a vehicle. If any device assigned to me and in my care is stolen from a public place and left unattended this could invalidate the insurance and I will be responsible for its replacement.

3. I agree to: treat the device with due care and keep it in good condition, ensure that it is strapped in to the carry case when transported and/or not in use, not leave the device unattended in class without being secured and avoid food and drink near the keyboard/touch pad.

4. When working on laptops I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the device malfunctioning.

5. I agree to only use software applications that are relevant to the work of the school. This includes cloud based application and software that has been downloaded onto any IT device.

6. I agree to not leave my device logged in and unattended at any location, including at home. I also agree to not permit persons other than school staff to have access the device and the potentially sensitive material it provides access to.

7. The school will ensure that Anti-Virus software is installed. It is my responsibility to ensure that this is kept up to date on a regularly basis by the school.

8. Should any faults occur, I agree to notify the school's ICT staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or any one other than ICT staff, attempt to fix suspected hardware, or any other faults.

9. I agree to attend training in how to access the Curriculum Network, Intranet and email within the school provided by IT staff.

10. I agree that home Internet access is permitted at the discretion of the Head Teacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.

11. I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.

12. I agree to adhere to School and LA policies regarding the following, updated as necessary:
    - Acceptable use,
    - Data protection/GDPR
    - Computer misuse,
    - Health and safety,
    - On-line safety policy,

Device Details

Product/ Make ………………………………… Model. ………………………………

Serial Number ……………………………….. School Code …BC60………….

Personnel Details

Loan Authorised by …………………………………

Head Teacher: ………………………..…………………. Date ……………………………….
(signature)

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

Name of Member of Staff …………………………….

Received by (signature): ……………………………. Date ……………………………

Any IT device in maintained schools may be covered by the West Sussex Local Authority insurance scheme. Machines in academies or free schools however will not be covered by this scheme. These establishments will have to make their own arrangements and amend clause 2 accordingly.

For any IT device to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the devices for theft (where there are signs of forced entry), and accidental or malicious damage. Those Schools who have opted for the additional Buildings and Contents policy will also receive cover for flood/water damage, storm damage etc. All equipment in Schools is automatically covered for fire, lightning and explosion.

All IT devices are not covered by the school policy:

- Whilst in vehicles,
- Left unattended in a locked household over 48 hours.

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to ICT staff. If stolen or damaged from an employee's home, County would first ask for a claim under the staff member's household policy. Claims from the School policy will only be made if this were unsuccessful.

Please note that regardless of the policy a stolen IT device is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

For General Insurance enquiries and claims contact Sharon Andrews or Lydie Butler from the Insurance & Risk Management team on 0330 2222 723.