



Staverton C.E Primary School

E-safety Policy

September 2020

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail as well as mobile learning, such as phones. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill. Young people have access to the Internet from many places, home, school, friends' homes, libraries and in some cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Principles

- Our e-safety policy has been written by the school, building on the Wiltshire e-safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.
- The school regards e-safety as extremely important and is committed to ensuring that all staff and children understand their responsibilities and provide regular information sessions to parents.
- The policy applies equally to staff, pupils, governors and all visitors to the school.

Created by: L Parsons

Date: September 2018

Approved

Review Date: September 2021

Authorised Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff.

- Staverton CE Primary School receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.

- Our home-school agreement includes the Responsible Use Policy and guidance for sound, image and video for web publication. (See The Wiltshire E Safety Toolkit).
- Staverton School's Internet access will be designed expressly for children's use and will include filtering appropriate to the age of the children.
- In the Early Years' Foundation Stage, access to the internet is likely to be by adult demonstration only. In Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- At Key Stage 2, children will be able to search the internet independently, using child-friendly, approved search engines, with the children being taught appropriate keywords with which to search. The children will be supervised at all times. Children will be taught what to do if they come across unsuitable and inappropriate materials so that these skills are embedded by the time they are using the internet independently.
- Parents will be informed that pupils will be provided with supervised Internet access (based on the example letter for primary schools in The Wiltshire E Safety Toolkit).

Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- A log of all staff with unfiltered access to the Internet will be kept and regularly reviewed.
- A designated member of the Senior Leadership team will review the popular permitted and banned sites accessed by the school.
- As a school, we will work in partnership with parents; Wiltshire Council, DFE and the SWGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites the URL (web address) and content must be reported to SWGfL (Tel: 0870 9081708) or email (abuse@swgfl.org.uk)
- Website logs will be regularly sampled and monitored.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head teacher, Safeguarding lead, LADO, Police, Internet Watch Foundation.
- Any material that we believe to be illegal must be referred to the Internet Watch.

Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Teaching and Learning

The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, pupils will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday life for education, business and social interaction. As a school, we have a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school. Therefore it is essential they learn how to evaluate Internet information and to take care of their own safety and security.
- Staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments.
- Educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to be critically aware of the materials they read and 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.
- If staff or pupils discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to the South West Grid for Learning
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

Communication and Content

Website Content

Many schools have excellent websites that inspire pupils to publish work of a high standard. Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs or videos of pupils are published on the school website/blog. Photographs/ videos will be selected carefully and will not enable individuals to be clearly identified.
- Pupils' names (first and/or surname) will not be used in association with photographs.
- Pupils' names and first letter of their surname will appear on the school blog.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Learning Platforms (N/A)

An effective learning platform (LP) or virtual learning environment (VLE) can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration.

- All users will be required to use an age appropriate password to access the relevant content of the LP which must not be shared with others.
- SLT and staff will regularly monitor the usage of the LP 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 LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.

- All users will be mindful of individual and intellectual property and will upload only appropriate content to the LP.
- When staff, pupils etc. leave the school their account or rights to relevant content areas will be disabled or transferred to their new establishment.

Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

Schools will need to determine the best approach for their circumstances, based upon pupil age and curriculum requirements. Pupils will only use their class email address (classname@staverton.wilts.sch.uk) when sending emails and responses should be viewed by the teacher to check appropriateness before being read by the pupils.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a responsible adult if they receive offensive e-mail.
- Staff will use official school provided email accounts.
- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is banned.
- Any document attachments which pertain to children must be encrypted before sending.
- Any portable devices that are linked to school email laptop/IPADs must be password protected.

If the school has to close due to COVID-19, teachers will use the class email addresses to communicate with parents. Parents are to only email class email addresses if the school is closed due to COVID. Parents are to email the admin address if they have a concern or want to communicate with a member of staff.

Blogging

Blogging involves pupils accessing blogs whilst in school and also at home. To be able to post, pupils need to log into the blog either using an individual sign in or a class sign in. The advantage of an individual sign in is that this gives more ownership to each pupil. A contributor can submit a post for review, however, this will need to be authorised by the Class Teacher before it appears on the blog. Everything that a pupil writes on the blog is moderated before it appears. Teachers will spend time in class discussing how to safely use the blog and how to comment on posts. This will be followed up in class over the academic year.

If there are any inappropriate comments that are attempted to be submitted, the Class Teacher will log this in the 'E-Safety incident log' and follow up with the children involved and the parents. The Senior Leadership Team will be informed and will take any further action if necessary. If any further attempts to post inappropriate materials reoccur, future posting will not be allowed and necessary sanctions will be carried out. Cyber bullying is taken extremely seriously at this school and we endeavour to implement the necessary learning experiences to ensure that children are not only safe whilst at school, but equipped to be responsible on the internet in their future years as an adult.

In addition, the following is to be strictly adhered to:

- Where services are “comment enabled”, comments are to be set to “moderated” this means that any post or comment will be read and approved by your child’s class teacher before it is posted on the school website.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Every pupil with a unique log in has been told to keep this private, if a pupil or parent thinks their log in needs changing, they should ask their child’s class teacher.

Class teachers will display the blogging rules in their classroom. They will discuss the rules (Appendix 3) with the children throughout the computing session. All adults in the school will follow the blogging rules (Appendix 2).

On-line communications and Social Media.

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.
- 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.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- 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.
- Parents are asked to carefully consider, before posting content on social media sites, whether it is appropriate to post certain content or if to do so would bring the school into disrepute, breach confidentiality or copyright or if it could be considered offensive, defamatory, discriminatory, bullying or is

potential harassment to an individual employed by the school. Where incidents of this nature are brought to the attention of the Senior Leadership Team, and they are deemed to be defamatory in some way, you will be invited into school to discuss the matter further and we may request that you remove the post or we may report abuse to the site involved.

- Parents wishing to photograph or video at an event should be made aware of the schools expectations and be required to comply with the schools RUP as a condition of permission to photograph or record.
- Concerns regarding students' 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 students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet access all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for schools to achieve. Due to the widespread use of mobile devices it is essential that schools take steps to ensure that these devices, both personally and school owned, are used responsibly and that they do not impede teaching and learning. Staff will be given clear boundaries on professional use.

The use of mobile phones and personal devices is a school decision, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Children and staff have access to resources to support learning and teaching
- Our school community will be given clear boundaries on responsible and professional use

These principles underpin our policy, which states that:

- Sending abusive or inappropriate messages or content is forbidden by any user within the school community

Policy for children

- Mobile phones that are brought in to school by children will be stored in the School Office during the school day. However, they remain the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.
- Children must not take mobile phones on school trips or residential visits unless agreed by the head teacher for medical reasons e.g. diabetes
- School staff authorised by the Head teacher may search children or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is

considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.

Policy for staff and visitors

Mobile phones that are brought into school by any member of staff or visitors must be stored remotely, away from the classrooms. Lockers are available for this purpose or they may be stored in the School Office during the school day. However, the school accepts no responsibility for the loss, theft or damage of such items.

- Staff mobiles will be turned off during teaching time, non- contact time and turned to silent during any staff or school led meeting.
- Personal electronic devices provided by the school may be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Where staff may need to contact children and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail or phone), unless under the direction of the headteacher e.g. residential. In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- During school hours, where family members may need to contact staff in an emergency situation, they should telephone the School Office in the first instance. Only in exceptional circumstances, and in agreement with the Head Teacher, will a member of staff be allowed to use a mobile phone during learning time.
- Staff will be provided with school equipment for the taking of photos or videos of children for educational purposes and will only use work-provided equipment for this purpose.
- Wherever possible, contractors will be asked to carry out maintenance outside of school hours. Where essential maintenance or emergency repair is required in teaching areas during school hours, all contractors will be supervised to comply with this policy.
- For the safeguarding of all involved, users must connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy
- A school mobile phone will be passcode protected and given to the designated Trip Leader to ensure confidentiality of mobile records.

Video Conferencing

Video conferencing (including FaceTime, Skype and Lync) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- Staff must refer to the internet consent agreements prior to children taking part in videoconferences.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised by the class teacher at all times when involved in video conferencing.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment should be completed on each new technology and assessed for effective and safe practice in classroom use.

The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Final approval will be with the Headteacher or Deputy.

Cyber Bullying

Many children and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that children, school staff and parents/carers understand how cyber-bullying is different from other forms of bullying. It is important to understand how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety within our school.

Cyber bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone” DCSF 2007. Examples of how cyberbullying may occur include via mobile phones, social networking sites, gaming, forums, email and sexting. The DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyber-bullying: <http://www.digizen.org/cyberbullying>. Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school’s behaviour, anti-bullying and child protection policies.

Cyber-bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school’s Anti-bullying and Child Protection policies, which include:

- Clear procedures are in place to investigate incidents or allegations of cyber bullying.
- Clear procedures are in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded and investigated by the designated Safeguarding Lead.
- 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.
- Children, staff and parents/carers will be required to work with the school to support the approach to cyber

Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act; this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact www.wiltshire.gov.uk

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Implementation

Policy in Practice - Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it is important to discuss the key features with pupils / students as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching will be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst children.
- Appropriate staff training will be completed annually.
- Online Safety teaching will be included in the curriculum and cover safe use at school and home.
- Online Safety rules will be on display in all classrooms and learning spaces with Internet access. A copy of the Responsible Use Policy will be available in the School Office.
- The SWGFL digital literacy curriculum scheme of work will be established across the school to raise awareness and importance of safety and responsible internet use amongst children.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Consultation with Staff on the Policy

It is important that all staff feel confident to use new technologies in teaching and the 'Online Safety' policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

All staff must understand that the rules for information systems misuse for Wiltshire Council employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

- The Online Safety Policy will be provided to and discussed with all members of staff and the Responsible Use Policy signed for compliance.
- Staff will be made aware that Internet traffic is monitored (and automatically reported by SWGfL) and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Policy in Practice - Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk. Schools may wish to refer parents to websites referred to in the references section of this document.

- Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy in newsletters, school prospectus and website.
- A partnership approach with parents and carers will be encouraged. This will include offering annual Online Safety updates alongside your children, as well as offering practical advice and resources to support safer Internet use at home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Parents will be informed if the School become aware of any children showing evidence of inappropriate use of the Internet at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure online safety is practised responsibly, both within school and at home.

Handling of complaints

Parents and teachers must know how and where to report incidents in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All records of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc.

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

This policy will be reviewed annually

Reviewed and Updated June 2016

Reviewed and Updated September 2017

Reviewed and Updated September 2018

Reviewed and Updated September 2019

Reviewed and Updated September 2020

Appendix 1

2020 Rules for Responsible Internet and Device Use for Adults



I will use all ICT equipment issued to me in an appropriate way, in line with the Online Safety policy.

I will not:

- Access offensive website or download offensive material.
- Make excessive personal use of the Internet or e-mail.
- Copy information from the Internet that is copyright or without the owner's permission.
- Place inappropriate material, or that which may impact negatively on the School community, onto the Internet.
- Send e-mails that are offensive or otherwise inappropriate.
- Disregard my responsibilities for security and confidentiality with regard to children's identities and data protection. Download files that will adversely affect the security of the laptop/IPAD and school network.
- Update web pages or use pictures or text that can identify the school and individual children.
- Attempt to repair or interfere with the components, software or peripherals of any IT equipment that is the property of Staverton C E Primary School.
- I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
- When emails relate to children within the school, I will encrypt any attachments sent and ensure that only initials are used for identification.
- Any removable media I use will be encrypted and free from any type of virus.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Online Safety Lead or IT technician.
- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
- I will report immediately to the Headteacher or Online Safety Lead any unpleasant material or messages sent to me.
- I understand that consequences will be taken if I deliberately access Internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden.
- I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop/IPAD removed and that other disciplinary consequences may follow.
- I agree to follow the Online Safety, in relation to the recreational use of social networking sites or other online technologies.
- My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Headteacher and register the passwords with the Headteacher.
- I will ensure I keep my network password secure and inform the Office Manager if this security is breached.

Signed: Date:

Appendix 2

Blogging rules for adults

The Role of the Blog Admin/Teacher:

The blog admin is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

1. Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!
2. If you use a shared computer, log out at the end of each session.
3. Promote the links on the class blog to the parents and the wider community. Twitter is a great way to promote a blog.
4. A blog can take a while to gather momentum and an audience. Be patient... the audience will come!
5. Your users will need to log in. For a quick solution, you can have one Username and Password for your class to get posts on the blog. However, for older pupils of 7+ they are more than capable of having their own log in.
6. EVERYTHING that people write on the blog is moderated before it appears. This means that a member of staff (class teacher) reads and checks things to decide if they are appropriate.
7. Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!
9. Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.

Any misuse of the Blog by staff or posting of inappropriate comments or materials will be treated as a disciplinary matter. Ultimately, it is up to each class teacher to ensure the safe and appropriate use of the Blog by their pupils.

Appendix 3



Rules for Responsible Internet Use for Children



These rules help us to be fair, responsible and keep everyone safe.

- I will ask permission before using the Internet and will only use the internet if there is an adult close by to supervise me.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school or use software or files from home.
- I understand that any mobile devices that I bring into school will be stored in the School Office.
- I will only e-mail and open attachments from people I know, or my teacher has approved, through the school system.
- Any messages I send will be polite and sensible.
- I understand that I must never post my home address, phone number or email address online, or arrange to meet someone.
- I will not use the Internet in school to access social media sites.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit and there may be consequences if anything inappropriate is found.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers and that my parents/carers may be informed.

I have read and understand the school rules for responsible internet use. I will use the computer system and internet in a responsible way and follow these rules at all times

Appendix 4

Blogging rules for Children

Don'ts:

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts

Do's:

1. Post about whatever you like.
2. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
3. Comment on other people's posts too. Blogging is about commenting and posting!
4. If your post doesn't appear straight away, your teacher might be busy, do be patient.
5. Try to post about things that your audience would like to read.
6. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
7. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
8. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.



Staverton C E Primary School

Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil:

Class:

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed:

Date:

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Please print name:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.

Signed:

Date:



Staverton CE Primary School

Sample Letter to Parents

1st September 2020

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Staverton CE Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, the South West Grid for Learning (SWGfL) operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely

Appendix 7

Staff Professional Conduct Agreement Laptop/IPAD policy for Staverton School staff



- The laptop/IPAD remains the property of Staverton School.
- The laptop/IPAD is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Staverton School Staff should use the laptop/IPAD.
- On the teacher leaving the school's employment, the laptop/IPAD must be returned to Staverton School on the last day of the term in which they leave. Staff on extended leave of 4 weeks and over should return their laptop/IPADs to the school (other than by prior agreement with the Headteacher).
- When in school and not being used, the laptop/IPAD must be kept in a safe place. It must not be left in an unlocked, unattended classroom.
- Laptops and IPADS must not be left in an unattended car, due to the confidential nature of the data. In exceptional circumstances, if there is a need to do so, it should be locked in the boot.
- The laptop/IPAD must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher, with evidence of adequate insurance.
- All software on laptops and IPADS must be fully licensed and have been installed by our IT technician, to ensure that no corrupt software or systems are installed.
- If any removable media is used, then it must be encrypted and checked to ensure it is free from any viruses.
- It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop/IPAD is kept up-to-date.
- Staff must use their laptop/IPAD in school on the network at least once a week to ensure virus protection is automatically updated.
- Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
- Staff should communicate with the School's IT technician with regard to technical issues, or the need to modify the laptops/IPADs.
- Students can only use the laptop/IPAD under the direct supervision of an adult.
- If any fault occurs with the laptop/IPAD, it should be referred immediately to the IT Technician.
- The laptop/IPAD would be covered by normal household insurance. If not it should be kept in school and locked up overnight.
- The purchase and installation of Apps on school IPADS must be agreed by Computing Coordinator and carried out by appropriately authorised members of staff (IT Technician).

The device I have is (Serial no.).

The device I have is (Serial no.).

I agree to adhere to this Conduct Agreement. Signed: Date:

Appendix 8

Web-based Resources

For Schools

KidSmart

<http://www.kidsmart.org.uk/>

SMART rules from Childnet International and Know It All for Parents

Childnet International

<http://www.childnet-int.org/>

Guidance for parents, schools and pupils

London Grid for Learning

<http://www.lgfl.net/lgfl/sections/safety/esafety/menu/>

Additional e-safety materials (posters, guidance etc.)

DfES Anti-Bullying Advice

<http://www.dfes.gov.uk/bullying/>

Internet Watch Foundation

www.iwf.org.uk

Invites users to report illegal Websites

South West Grid for Learning – Safe

www.swgfl.org.uk/safe

A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know?

www.thinkuknow.co.uk/

Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

For Parents

Kids Smart

<http://www.kidsmart.org.uk/parents/>

A Parent's guide to Internet devices

Childnet International

<http://www.childnet-int.org/>

"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

E-safety page on School website

<http://www.staverton.wilts.sch.uk/e-safety-1/>

Useful contact details: South West Grid for Learning (SWGfL)

Support Team - (including the registering of inappropriate content needing to be filtered).

Telephone: 0870 9081708

E-mail: support@swgfl.org.uk

To notify of an inappropriate website: abuse@swgfl.org.uk