West Wittering Parochial Church of England Primary School

Acceptable Use and E Policy Merged Document

Document Name

1. Model Acceptable Use Policy for SIMS Learning Gateway Users
2. Model Staff Acceptable Use Policy
3. Model Students KS1/KS2 Acceptable Use Policy
4. Example Parent Permission Letter
5. Model E-Safety Policy
6. E-safety Incident Procedures
7. Email address sharing letter – example
8. ICT in schools checklist;
9. Internet Security and Safety guidance;
10. Staff Permission Form.
11. BYOD Agreement (Bring Your Own Device) Agreement

West Wittering Parochial Church of England Primary School

Acceptable Use Policy for the SIMS Learning Gateway

Parents and carers of pupils at West Wittering Primary School are able to obtain online access to the School's Information Management System (SIMS) via the **Sims Learning Gateway** (SLG). Through this website, parents and carers can access information produced by the school about their child/ren via a secure Internet connection.

This policy applies to **all** those who access the West Wittering Primary School SIMS Learning Gateway system (thenceforth referred to as the "SLG system"). This policy applies whenever and wherever information is accessed, whether the computer equipment used is owned by West Wittering Primary School or not.

Access is granted strictly on condition that the individual formally agrees to the terms of this Policy through the return slip attached to the letter accompanying this policy.

Authorised SLG Users
Only relevant members of staff and persons who are legally responsible for student(s) currently attending the school are provided with online access to the West Wittering Primary School SLG system. Even then they only have access to information relating to the students where they have that legal responsibility.

Requests for access to the "SLG system" must be made to West Wittering Primary School using the SLG Parental Access Return Slip. The authorising member of school staff and the parent/guardian/carer concerned **must** confirm that there is a legitimate entitlement to access information for the student(s). The name(s) of the student(s) must be stated on the SLG Parental Access Letter and the accompanying return slip.

The school, for audit purposes, will hold a copy of the letter, with the corresponding signed return slip. It is important to manage access to the schools SLG system effectively. The school is required to arrange the removal of access of users who are no longer entitled to access to that SLG within 1 week of being informed of that change in status.

Acceptable Use of the SIMS Learning Gateway – All Users

- Access to the SIMS Learning Gateway is a privilege, not a right. Users are responsible for their behaviour.

- Conditions of use are respected: any breach of the conditions of use may lead to withdrawal of a user's access. In some instances, such a breach could lead to criminal prosecution; in the case of staff it may be considered a disciplinary matter.
- The system should not be used in any way that might bring the name of the school or County Council into disrepute.
- Staff, parents and students are expected to use the resources for the purposes for which they are intended.
- All users accept personal responsibility for reporting any misuse of the system to a teacher or to a member of the school technical team.
- No user should access, create, transmit, display or publish any material, including images and data from the "SLG system", which is likely to cause offence, inconvenience or needless anxiety.
- No user should create, transmit, display or publish any material, including images and data from the "SLG system" that might be considered defamatory.
- Staff, parents and students should not make unauthorised attempts to access data and resources on the "SLG system" by bypassing security or password protections.
- No user should take any action designed or likely to cause corruption or destruction of other users' data, or violate the privacy of others.
- Users should inform the School Technical Support Team immediately if a security problem is identified. They should not demonstrate this problem to other users.
- Users should inform the School Technical Support Team immediately if they appear to have access to content that is not authorised. They should not demonstrate this problem to other users.

Acceptable Use of the SIMS Learning Gateway – Staff Only

- Protection of information – be aware of the Data Protection Act. Only place information within a student's record that a person with a legal responsibility for that student has a right to see.
- Sharing of information - be aware of the Freedom of Information provisions. Write only that which may be scrutinised without embarrassment to writer or recipient.
- Members of staff, as representatives of the school community, must remember to enter only appropriate content and use only appropriate language when using the system.

Information Security

This Policy is intended to minimise security risks. These risks might affect the integrity of West Wittering Primary School data, the Authorised SLG User and the individuals to which the SLG data pertains.

Information made available through the SLG system is confidential and protected by law under the Data Protection Act 1998. In order to comply with this Act:

- Users must not distribute or disclose any information obtained from the SLG system to any person(s) with the exception of the student to which the information relates or to other adults with parental responsibility for that student. Users should not attempt to access the SLG system in any environment where the security of the information contained in the SLG system may be placed at risk such as an Internet café or public place.
- Users must not transfer information from the SLG system to any form of portable media such as pen drives or by electronic means such as e-mail without the express permission of the school
- Passwords for SLG accounts should be complex and consist of at least six characters including a combination of capital letters, lower case letters and numbers. Ideally, at least one symbol should be included as well.
- Users must always keep their individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Never use anyone else's username or password.
- If you think someone has learned your password then contact the School Technical Support Team in school or change it immediately if possible.

Denial 0f Access
Users are liable for any potential misuse of the system and/or breach of the Data Protection Act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

West Wittering Primary School reserves the right to revoke or deny access to the SLG system of any user under the following circumstances:

- If the validity of parental responsibility is questioned.
- A Court ruling preventing access to child or family members is issued.
- Where a user or users are found to be in breach of the SLG Acceptable Use Policy.
- If any child protection concerns are raised or disputes occur the school will suspend access for all parties concerned pending investigation.
- If a user is identified as a security risk.

Please Note: Where access to the "SLG system" is not available West Wittering Primary School will still make the information available but only in a manner permitted by The Data Protection Act (1998).

Enquiries
SLG users should forward any enquiries or complaints about the West Wittering Primary School SIMS Learning Gateway system to Mrs Sue O'Boyle, head@westwittering.w-sussex.sch.uk or by telephone 01243 513015.

West Wittering Parochial Church of England Primary School

Staff Acceptable Use Policy

School networked resources, including SIMS Learning Gateway and Moodle, 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 the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and/or retrospective investigation of the users use of services; and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

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 Mrs Sue O'Boyle.

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 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 students.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are 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 and/or contact Mrs Sue O'Boyle.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username, I will **not** continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that email 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 use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to Mrs Sue O'Boyle.
15	I will not use "USB drives", portable hard-drives, "floppy disks" or personal laptops on the network without having them "approved" by the school and checked for viruses.
16	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.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images – I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such as school parents and their children.
19	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.
20	I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.

21	I will not send or publish material that violates the Data Protection Act or breaches the security this act requires for personal data, including data held on the SIMS Learning Gateway.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

Additional guidelines

- Staff must comply with the acceptable use policy of any other networks that they access.
- Staff will follow the "Safer Use Of The Internet By Staff Working With Young People" published within the West Sussex Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP

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 Mrs Sue O'Boyle 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 by Mrs Sue O'Boyle. 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 students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc.) if written parental consent has been given.

Further guidance can be found in the "Model Policy for schools regarding photographic images of children" August 2010.

Copies can be obtained from section 6 of the WSSS Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult Mrs Sue O'Boyle.

I agree to report any misuse of the network to Mrs Sue O'Boyle.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to Mrs Sue O'Boyle.

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 Mrs Sue O'Boyle.

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: _____

Staff Signature: _____

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

West Wittering Parochial Church of England Primary School

Pupil Acceptable Use Policy

All pupils must follow the rules in this policy when using school computers.

Pupils 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. Their teachers will show pupils how to use the computers.

	Computer Rules
1	I will only use polite language when using the computers.
2	I must not write anything that might upset someone or give the school a bad name.
3	I know that my teacher will regularly check what I have done on the school computers.
4	I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5	I must not tell anyone my name, where I live, or my telephone number over the Internet.
6	I must not tell my username and passwords to anyone else but my parents.
7	I must never use other people's usernames and passwords or use computers left logged in by them.

8	If I think someone has learned my password then I will tell my teacher.
9	I must log off after I have finished with my computer.
10	I know that e-mail is not guaranteed to be private. I must not send unnamed e-mails.
11	I must not use the computers in any way that stops other people using them.
12	I will report any websites that make me feel uncomfortable to my teacher or another member of staff.
13	I will tell my teacher or another member of staff straight away if I am sent any messages that make me feel uncomfortable.
14	I will not try to harm any equipment or the work of another person on a computer.
15	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.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Waste time or resources on school computers.

✂ -

Student User Agreement Form for the Student Acceptable Use Policy

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 also agree to tell my teacher or another member of staff if I see any websites that that make 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/Carers/Guardians Name: ____

Parent/Carers/Guardians Signature: ________________________________

Date:___/__ /_____

West Wittering Parochial Church of England Primary School

04/02/2015

Dear Parents

As part of the school's ICT programme, we offer pupils supervised access to the Internet. Before being allowed to use the Internet, we require all pupils to obtain parental permission. Access will only be given if both **you** and **your child** sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and other information plus exchange messages with other Internet users throughout the world. Every effort will be taken by the school to ensure that pupils are only able to access suitable information sources. The school Internet Service Provider operates a filtering system that restricts access to inappropriate materials. However, families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive. Whilst our aim for Internet use is to further educational goals and objectives, it is always possible that pupils may find ways to access other materials. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

We recognise that parents and guardians of minors have the ultimate responsibility for setting and conveying the standards that their children should follow. We also appreciate this is exercised on a daily basis through the control you exert over your child's access to information sources such as television, telephones, films, radio and other media. During school time, teachers will exercise equal vigilance in guiding pupils only towards appropriate material. However, the school supports and respects each family's right to decide whether or not to apply for access.

We should be grateful if you would read the enclosed documents. If you wish your child to have access to the Internet at school, please complete the permission form and return to the school office.

Thank you in anticipation for your co-operation in this matter.

Yours sincerely

Mrs S O'Boyle

E-Safety Policy For Schools

Introduction

Our aim in presenting an e-safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.

E-safety is not purely a technological issue. The responsibility for e-safety must not be solely delegated to technical staff, or those with a responsibility for ICT.

Schools must therefore, firmly embed e-safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

No one policy or technology can create the safe learning and working environment we need. Schools can work towards this by combining the following:

1. **Policies** and Guidance.
2. **Technology** Based Solutions
3. **Education** in terms of acceptable use and responsibility

Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

☐ The school Acceptable Use Policy (AUP)
☐ The school / academy Internet Filtering Policy
☐ The staff Guidance for the Safer Use of the Internet
☐ The Information Security Guidance

These policies set the boundaries of acceptable use. Schools need to use these policies however in conjunction with other policies including, but not limited to:

☐ The Behaviour Management Policy
☐ The Anti Bullying Policy
☐ The Staff Handbook / Code of Conduct for Staff

Technology

The technologies to help form a safe environment to learn and work include:

☐ Internet filtering – The West Sussex Capita Partnership (WSCP) provides a system (OpenHive-Webshield) for those schools and academies on the schools network. Establishments not on the schools network will provide their own internet filtering solution.

☐ Antivirus Software – regularly updated and may be supplied by the Schools IT Support Team (SITST).

☐ Schools may also decide to use "Automatic network monitoring software" including, but not limited to, products such as Securus or Policy Central.

Education

The education of young people is key to them developing an informed confidence and resilience that they need in the digital world.

The National Curriculum programme for ICT at Key Stages 1 to 4 makes it mandatory for children to be taught how to use ICT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and the professionals who come into contact with children.

Educating young people in the practice of acceptable use promotes responsible behavior and builds resilience. Personal, Social and Health Education (PSHE) lessons can also provide an opportunity to explore potential risks, how to minimize these and to consider the impact of our behaviour on others.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, young people must be able to transfer established skills and safe working practices to any new "e-activities" they encounter.

We recognise that it is equally important to ensure that the people who care for young people should have the right information to guide and support young people whilst empowering them to keep themselves safe.

The 360° safe - the e-safety self-review tool

The 360° safe self review tool is currently available free of charge and provided by the South West Grid for Learning. It is intended to help schools review their e-safety policies and practice and provide the following:

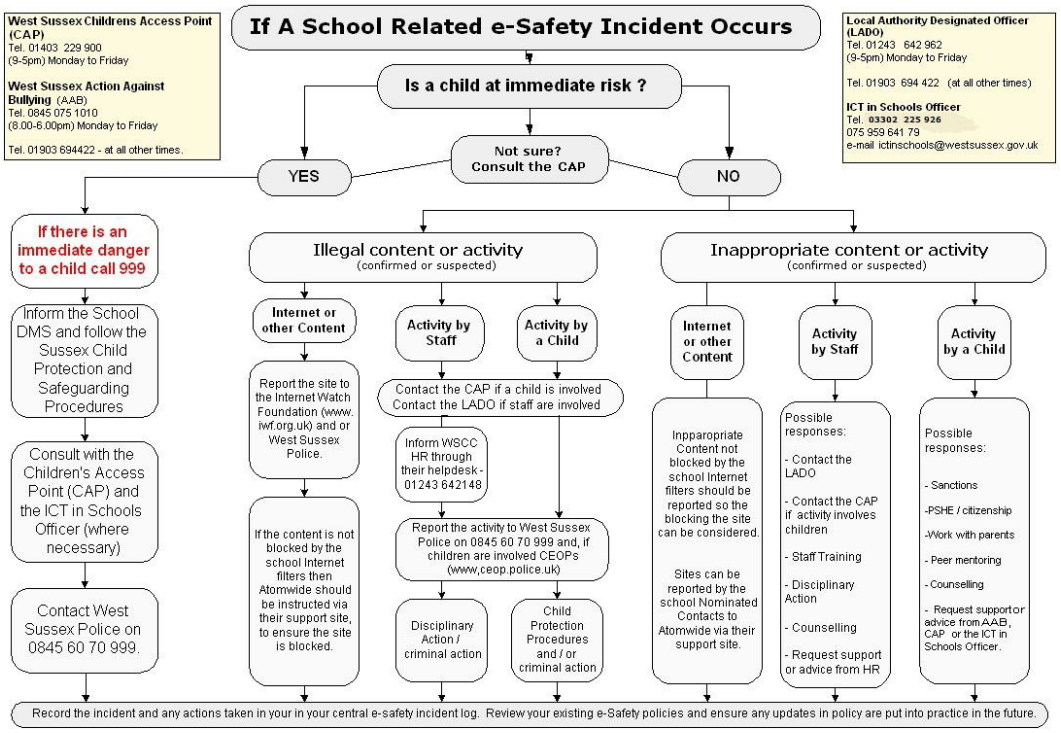
☐ Management information that can help the production or review of e-safety policies and develop good practice.

☐ A process for identifying strengths and weaknesses in your schools policies and practices.

☐ Opportunities for commitment and involvement from the whole school.

☐ A platform for schools to discuss how they might move from a basic level provision for e-safety to practice that is aspirational and innovative.

If you have any queries please contact either Simon Gawn, ICT in Schools Officer, on 03302 225 926 or email ictinschools@westsussex.gov.uk


West Sussex Childrens Access Point (CAP)
Tel. 01403 229 900
(9-5pm) Monday to Friday
West Sussex Action Against Bullying (AAB)
Tel. 0845 075 1010
(8.00-6.00pm) Monday to Friday
Tel. 01903 694422 - at all other times.
If A School Related e-Safety Incident Occurs
Local Authority Designated Officer (LADO)
Tel. 01243 642 962
(9-5pm) Monday to Friday
Tel. 01903 694 422 (at all other times)
ICT in Schools Officer
Tel. 03302 225 926
075 959 641 79
e-mail ictinschools@westsussex.gov.uk
Is a child at immediate risk ?
Not sure? Consult the CAP
YES
NO
If there is an immediate danger to a child call 999
Inform the School DMS and follow the Sussex Child Protection and Safeguarding Procedures
Consult with the Children's Access Point (CAP) and the ICT in Schools Officer (where necessary)
Contact West Sussex Police on 0845 60 70 999.
Illegal content or activity
(confirmed or suspected)
Inappropriate content or activity
(confirmed or suspected)
Internet or other Content
Activity by Staff
Activity by a Child
Report the site to the Internet Watch Foundation (www.iwf.org.uk) and or West Sussex Police.
If the content is not blocked by the school Internet filters then Atomwide should be instructed via their support site, to ensure the site is blocked.
Contact the CAP if a child is involved
Contact the LADO if staff are involved
Inform WSCC HR through their helpdesk - 01243 642148
Report the activity to West Sussex Police on 0845 60 70 999 and, if children are involved CEOPs (www,ceop.police.uk)
Disciplinary Action / criminal action
Child Protection Procedures and / or criminal action
Internet or other Content
Activity by Staff
Activity by a Child
Inpparopriate Content not blocked by the school Internet filters should be reported so the blocking the site can be considered.
Sites can be reported by the school Nominated Contacts to Atomwide via their support site.
Possible responses:
- Contact the LADO
- Contact the CAP if activity involves children
- Staff Training
- Disciplinary Action
- Counselling
- Request support or advice from HR
Possible responses:
- Sanctions
-PSHE / citizenship
-Work with parents
- Peer mentoring
- Counselling
- Request support or advice from AAB, CAP or the ICT in Schools Officer.
Record the incident and any actions taken in your in your central e-safety incident log. Review your existing e-Safety policies and ensure any updates in policy are put into practice in the future.

West Wittering Parochial Church of England Primary School

Dear Parents,

In Year __ we are currently teaching the students how to send, receive and reply to emails. In order to practise and develop this skill we have the opportunity to pair up with another school and for the students to have an 'email buddy'. The children will be able to ask and answer questions about themselves, their school and the topics they are working on. The school involved is _ _ _ _ _ _ _ in _ _ _ _ _ __ _ _ _.

In order to make this possible each student has an email account set up at school. Each student has a user name and password that only they can use. We will need to pass the e-mail address of each student involved on to the school we are pairing with. Along with this information we will also need to send each student's full name and class details.

To ensure the safety of all involved in this project the student at both schools will be supervised at all times and will follow their schools 'Acceptable Use Policy'. You will have received a copy of this when your child started at _ _ _ _ _ _ _ School and your child will have a signed copy of this on their records.

If you are happy for your child to participate in this project and for their email address details to be passed onto <*nominated member of staff*> please complete the slip below.

We hope your child will enjoy this exciting opportunity.

Yours sincerely

I give permission for my child's email address details to be passed onto <*nominated member of staff*>.

Child's name _____ Child's class _____

Signature _____ Date _____

West Sussex Schools Acceptable Use Policy

ICT in Schools Checklist

Version 1.1

Title : ICT in Schools

File Name : ICT in Schools v1.1.doc

Synopsis : This document forms part of the West Sussex County Council Schools Acceptable Use Policy and specifically relates to the implications of ICT in School's.

Current Issue:

Status : Published.

Version Number : 1.1

Issue Date : 12/10/2009

Author : Simon Gawn

Changes History:

Issue No.	Date	Author	Principal Changes
1.0	02/10/2009	Simon Gawn	Original material was taken from V4.9 of the original; Web based AUP to form a downloadable document.
1.1	22/08/2013	Simon Gawn	Minor cosmetic changes and adding a copyright notice to the footer

15. ICT in Schools Related Checklist

- Does the school have an Acceptable Use Policy (AUP) that is regularly updated to take account of emerging technologies?

- Does the school ensure that members of staff undertake to secure portable ICT equipment such as laptops and cameras when not in use? Are sanctions in place where staff fail to do so resulting in loss of equipment?

- Is pupils' use of the Internet, email and/or chat rooms regularly monitored to ensure that inappropriate use is not being made? Are sanctions in place where pupils access inappropriate sites or post bullying or offensive messages?

- Have pupils and parents been advised that pupils' use of the Internet and e-mail systems may be monitored?

- Does the school send information to parents regarding ICT use in schools?

- Have all pupils and parents/carers (where appropriate), including mid term entrants, given their consent for children to use the Internet in school? What action will the school take if consent is withheld?

- Does the school employ the use of biometrics such as fingerprint recognition in library/registration/school meals systems? If so, does the school comply with the Data Protection Act (1998) in the processing of students data? Has the school gained parental consent for the use of the system?

- Does the school have filtering systems in place to prevent pupils from accessing inappropriate materials? Are there procedures in place for pupils to report accidental access to inappropriate material?

- Does the school adopt safe practices regarding the publication of the images and names of pupils and staff on its website?

- Does the school take reasonable measures to monitor the use of emails by pupils and staff?

- Does the school provide appropriate opportunities within a range of curriculum areas to teach Internet safety?

- Are there procedures in place to deal with 'disclosure' by a child of a personal nature as a result of Internet safety education? Has the school

nominated a member of staff who has responsible for such issues?

- Does the school ensure that Anti Virus Software is installed on all machines within the school? Does the school ensure that this software and its windows operating systems are regularly updated?

- Has the school deployed an appropriate level of security on its networks to ensure their reliability and prevent unauthorized access to systems and data?

- Does the school have an Information Security Policy to ensure that the information that it holds, is accurate, available and secure. This is perhaps especially important on portable devices such as laptops and USB memory sticks

- Has the school deployed sufficient security on any wireless networking to ensure that there is no unauthorized access to the school network and so the West Sussex wide area network?

- Does the school possess sufficient software licences for the software installed on its network?

West Sussex School Acceptable Use Policy

Section 03. Internet Security & Safety

Version 1.1

Title : **Internet Security & Safety**

File Name : Internet Security & Safety v1.1.doc

Synopsis : This document forms part of the West Sussex County Council Schools Acceptable Use Policy and specifically relates to the implications of the Data Protection Act in school.

Current Issue:

Status : Published.

Version Number : 1.0

Issue Date : 12/10/2009

Author : Simon Gawn & Mandy Stevens

Changes History:

Issue No.	Date	Author	Principal Changes
1.0	24/12/2009	Simon Gawn	Original material was taken from v4.9 of the original; Web based AUP to form a downloadable document.
1.1	19/08/2014	Simon Gawn	Updates following the move to OpenHive for many schools.

Contents

1. Action for Schools - Internet Use

Most pupils are very familiar with Internet use and culture so it would be wise for schools to discuss the school policies that relate to its use with them. This discussion may possibly be through a student council. As pupils' perceptions of the risks will vary, the rules may need explanation and discussion. Pupils may need to be reminded of the school rules at the point of Internet use.

Formatted: Font color: Auto

Formatted: Font color: Auto

- Rules for Internet access will be posted in all rooms where computers, or mobile devices are used.
- Parents of new entrants and, if appropriate pupils, will be asked to sign and return a consent form for Internet access. This must include mid-year entrants. (See Examples of letters, permission forms and posters within the Schools AUP)
- Pupils and staff will be informed that Internet use will be monitored and if needs be traced to the individual user.
- Schools may place Pupils and Staff that are under reasonable suspicion of misuse under retrospective investigation. Alternatively schools may actively monitor users suspected of misuse. This misuse may be in terms of time or content.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the PSHE programme covering both school and home use.
- Staff and pupils should inform the member of staff responsible immediately if a security problem is identified. Do not demonstrate this problem to other users.
- Users must login with their own user ID and password, where applicable, and must not share this information with other users with the exception of students asked to share their login details with their parents / carers so they can access the schools Virtual Learning Environment – for example Moodle, at home.
- Users identified as a security risk will be denied access to the network.
- Methods to identify, assess and minimise risks will be reviewed regularly.

The school will keep an up to date record of all staff and pupils who are granted

Internet access. For instance a member of staff may leave or a pupil's access be withdrawn. Those managing school networks need up to date lists of current staff and pupils who are to be given access. In addition to this they will need to be informed of staff or pupils leaving so there accounts can be at first disabled and ultimately deleted.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

The member of staff responsible will ensure that the Internet policy is implemented and compliance with the policy monitored.

2. Misuse of the Internet

Misuse of the Internet service provided by the School includes but is not limited to:

- Searching for or making, sending, displaying or publishing any material (e.g. imagery, sound or information) that is likely to cause offence, inconvenience, needless anxiety and/or bring the school into disrepute.
- Searching for / looking at, making or publishing offensive material.
- Receiving, publishing or sending material that breaks Copyright Law or the Data Protection Act.
- Sending unsolicited material to other users (including those on other networks)
- Trying to look at data and resources on the school office network system or other systems outside school unless permission has been granted.
- Acting in a way that would cause corruption or destruction of other users' data, violate the privacy of other users or intentionally waste time or resources on the school system or elsewhere.
- Downloading software without the approval of the *member of staff responsible*.
- Spending excessive amounts of time using the Internet (including via mobile devices) for non-school/work related reasons. (Incidental personal use is permitted provided it complies with these protocols and does not interfere with work or study).

Failure to adhere to these protocols may result in loss of access to the Internet as well as other disciplinary action.

3. Other Considerations

- Being polite and never sending, or encouraging others to send, abusive messages. Defamatory comments could result in legal action. E-mail has been used successfully as evidence in libel cases.

- Using appropriate language. Users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.

- 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 should not be sent. The school reserves the right to apply monitoring arrangements in relation to e-mail use where misuse is suspected.

- Not using the Internet in any way that would disrupt the use of the network by others. The school reserves the right to apply monitoring arrangements to any student or member of staff in relation to Internet use and related services where misuse is suspected.

4. The Purpose of Monitoring or the Investigation of Users

- To ensure compliance with the schools Acceptable Use Policy
- To investigate unauthorised use of the Internet and e-mail systems.
- To protect the operational availability and performance of ICT technical infrastructure.
- To continue the work of a school if an addressee is absent.
- To comply with the County Council's or Academy Trust's statutory obligations.
- To prevent or detect crime.

5. Filtering

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take 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 or its Internet Filtering provider can accept liability for the material accessed, or any consequences of Internet access.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Internet content. Filtering may be performed by:

- Internet Service Provider
- West Sussex Capita Partnership (OpenHive)
- School-level systems
- or, any combination of the above

School-level systems require considerable management to maintain effectiveness and place huge responsibility on the school if they are the only systems in place.

Careful monitoring and management of all filtering systems will be required. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

6. Action for Schools - Filtering

- The school will work in partnership with parents, the Local Authority, DfE and the Internet Service Provider to ensure that the Internet filter systems protect pupils and are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL (website address) and content must be reported to the Internet Service Provider via the nominated contact / *member of staff responsible.*

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Headteachers having reasonable suspicion that a member of staff is misusing the system should consult with their HR Business Partner to obtain guidance before instigating an investigation into e-mail or Internet Access misuse.

West Wittering Parochial Church of England Primary School

Staff User Agreement Form for Internet Access

As a school user of the Internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. I agree to report any misuse of the network to Mrs Sue O'Boyle. I also agree to report any websites that are available on the school Internet that contain inappropriate material to Mrs Sue O'Boyle. 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 Mrs Sue O'Boyle.

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: _____

Staff Signature (if appropriate): _____

Date: _____/_____/_____

West Wittering Parochial Church of England Primary School

Bring Your Own Device (BYOD) Agreement

Please read and sign the agreement below. No student will be permitted to use personal technology devices unless the agreement is signed and returned to show that you both understand and accept the terms of the agreement. The agreement is made between the pupil (please insert pupil's name) …….. and West Wittering Primary School.

Students wishing to use their personal devices on the West Wittering Primary School site must also adhere to its: Student Code of conduct; Internet Acceptable User Policy; and Anti-Bullying policy. Please read carefully and initial every statement to show that you both understand and accept each one as part of this agreement:

Statements	**Initial**
1. I am fully responsible for my device(s). I understand that West Wittering Primary School is not responsible for the device(s) in any way.	
2. I am not permitted to leave my personal device(s) at West Wittering Primary School outside of "school hours".	
3. When not in use for educational purposes my device(s) must be left "on silent" to prevent any disruption and be put away when asked to by teachers.	
4. I must immediately comply with any teacher's requests to shut down or close the screen on my device(s).	
5. I understand that I am not permitted to either transmit or upload photographic images/videos of any person on the West Wittering Primary School campus to the Internet other than school approved sites.	
6. I am responsible for charging my personal device(s) before bringing it/them to school so it/they can run on their batteries whilst at school. Charging may not always be available and it will always be at the discretion of teachers.	
7. I understand that West Wittering Primary School will not accept any responsibility for damage to my devise under any circumstances including damage caused by connecting to the school network and any infection by malware.	
8. To ensure appropriate Internet filters are in place, I understand that I can only use West Wittering Primary School's WiFi connection in the school site and will not attempt to bypass the network restrictions by using a 3G or 4G network.	
9. I understand that I must take all reasonable steps to avoid bringing devices onto West Wittering Primary School premises that might infect the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information. Failure to do so is in violation of the Acceptable Use Policy and will result in disciplinary action in accordance with the Schools Behaviour Policy.	
10. I accept that West Wittering Primary School has the right to examine any device that is suspected of causing problems or is the source of an attack or virus infection.	
11. I accept that printing from my personal device(s) is permitted only at the discretion of teachers.	

12. I understand that I must not physically share my personal devices with other students, unless I have written parental permission to do so.	
13. I agree that my device(s) cannot be used during assessments of any kind unless otherwise specifically directed by a teacher.	

I understand that the use of personal device(s) on the West Wittering Primary School site is only permitted in so far as it supports my educational experience. It is not a right but a privilege, and I understand that any breach of these rules may result in the removal of this right at any time and without notice. I also understand that any breach of these rules may result other disciplinary action.

I confirm that I understand and agree to follow the above rules and guidelines.

Student's name (printed) _____

Signature of Student _____

Date ____/____/20____