Westbury- on-Severn C of E Primary School
Acceptable Internet Use Policy

Internet use includes accessing the World Wide Web and the use of electronic mail.

1.0 Pupil access to the Internet

- The school encourages use by pupils of the Internet, together with the development of appropriate skills to analyse and evaluate resources found on it. These skills will be fundamental in the society our pupils will be entering. We also believe the Internet can give our pupils access to a huge variety of information which will stimulate and enrich their learning.
- In order to match electronic resources as closely as possible to the national and school curriculum, teachers will review and evaluate resources in order to offer web addresses and menus of materials that are relevant and appropriate to the learning objectives, age range and ability of the group being taught.
- The school expects that staff will investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the appropriate use of such resources.
- When necessary, Staff will consult the ICT co-ordinator for advice on content, training and appropriate teaching levels consistent with the school's ICT scheme of work and ICT strategy.
- Staff seek to organise information resources in ways that point pupils to those that have been reviewed and evaluated prior to use. Staff must remain vigilant when their pupils are using the Internet in order to ensure that offensive materials are not accessed.
- We acknowledge that access to the Internet can open classrooms to electronic information resources that have not been approved by teachers as appropriate for use by pupils. As with printed materials, the parents and guardians of minors are ultimately responsible for setting and conveying the standards that their children should follow when using media and information sources. Individual users of the Internet are responsible for their behaviour and communications over the Internet. It is presumed that users will comply with the school rules regarding use of the school network and will honour the agreements they have signed. (See Appendix 2)
- All pupils will be informed by staff of their rights and responsibilities as users either as an individual user or as a member of a class or group. Independent pupil use of the Internet will only be permitted upon submission of permission and agreement forms signed by parents of pupils and by pupils themselves. Permission is not transferable and may not be shared.
- The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages of the Internet. To that end, the school supports and respects each family's right to decide whether or not to grant access.
- School staff will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.
- Sending messages by e-mail will only be undertaken as part of a whole class or group project, with the knowledge and supervision of the class teacher.

2.0 Managing use of the Internet

- The school maintains students will have supervised access to Internet resources (where reasonable)
- Staff will preview any recommended sites before use.
- If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

3.0 Staff access to the Internet

- School staff have access to the Internet for preparation of materials and the exchange of information for professional purposes. While personal use of the Internet in their own time is permitted, staff should refrain from downloading any material in breach of copyright (or any other) law or of such a size as to take up an unreasonable amount of space on our server. The school will provide a secure e-mail address to all members of staff requesting one. All users of the network must be aware that their user area, including their internet use history, may be accessed by network administrators.

4.0 School Procedures

4.1 Personal Mobile devices (including phones)

- The school does not permit children to come to school with mobile phones and devices for their own use.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device e.g. In cases of emergencies such as field trips.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- No images or sound recordings may be made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

5.0 Using cameras and video cameras. **Taking of images and film**

- Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

6.0 Pupil Guidelines for Computer Use

- Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor.
- Staff may review files and communications stored in User Areas to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.
- The Internet is provided for pupils to conduct research and communicate with others when appropriate. Parents' permission is required. Access is a privilege, not a right and that access requires responsibility.
- Individual users of the Internet are responsible for their behaviour and communications over the network.
- Users are expected to comply with school standards and to honour the agreements they have signed.
- During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance.
- Pupils are protected whilst using the internet by internet security. This security is in the form of 'Hector the Protector'. Children will learn how to use the internet safely and how to safeguard themselves from inappropriate material. If such material is accessed by the pupils, then they will be taught the procedures for reporting and dealing with it.

7.0 e-Safety skills development for staff

- Our staff receive information and training on e-Safety issues in the form of staff meetings and notices.
- Details of the ongoing staff training programme can be found from the ICT co-ordinator**.**
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community. Matters of child protection will be reported to the head teacher immediately.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

8.0 e-Safety in the Curriculum

- School internet access is controlled and regularly monitored by Gloucestershire County Council's web filtering service, SWGFL. Pupils are taught about 'Hector the Protector' and how to use him safely if they should come across inappropriate internet material.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies. (See Anti-bullying Policy)

9.0 Managing the school e-Safety policy

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.

10.0 School Rules

- The school has developed a set of guidelines for Computer Use including the use of the Internet. These rules will be made available to all pupils, and kept under review. (Appendix 5)
- All members of staff are responsible for explaining to pupils the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

11.0 Rules to be shared with pupils:

- Always log onto the network using your own username.
- If passwords are required, these must never be communicated to anyone else.
- Always quit from programs properly and log off the network safely.
- Stick to the task you have been given to do.

The following are **not permitted**, especially when using the Internet:

- Using the internet without adult supervision
- Using websites that have not been approved by the class teacher

- Searching for, downloading, sending or displaying offensive messages or pictures
- Using bad language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using others' passwords
- Trespassing in others' folders, work or files
- Intentionally wasting limited resources (such as printers)

12.0 Rules for children when using E-mail

- I will only e-mail people I know or my teacher has approved
- I will only send messages which are polite and responsible
- I will not give my home address or telephone number or arrange to meet someone unless my parent, carer or teacher has given permission.
- I will never communicate with someone, or respond to emails from someone I don't know.

13.0 Sanctions

- Breaking the above rules will result in a temporary or permanent ban on computer or Internet use.

Misuse and Infringements

14.0 Complaints

- Complaints relating to e-Safety should be made to the ICT co-ordinator or Headteacher. Incidents should be logged and the **Flowcharts for Managing an e-Safety Incident** should be followed (see appendix 3).

15.0 Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart Appendix 4.1 & 4.2.)
- Users are made aware of sanctions relating to the misuse or misconduct on the **Acceptable Use Agreement**

Equal Opportunities

16.0 Pupils with additional needs

- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Writing and Reviewing this Policy

17.0 Staff and pupil involvement in policy creation

- Staff have been involved in making/ reviewing the e-Safety policy through staff meetings.
- Staff, Governors and visitors to the school engaged in Internet use will be expected to sign a copy of this policy signifying agreement to abide by the rules laid down herein. (Appendix 1)

18.0 Review Procedure

- There will be an on-going opportunity for staff to discuss with the ICT coordinator any issue of e-Safety that concerns them.
- This policy will be reviewed every12 months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix 1

Westbury-on-Severn CE Primary School

Acceptable Use Agreement/Code of Conduct: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT / e-Safety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without seeking permission from the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will not communicate with pupils of this school via Facebook or any other social networking site.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….……. Date ……

Full Name …….....(printed)

Job title . . . . . .……..

Westbury-on-Severn CE Primary School

Pupil Acceptable Use Agreement / e-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use the school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will click on Hector and tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I will not communicate with any school staff via Facebook or any other social networking site.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Signed: (Child)…….. (Parent) ……

Printed Full Name: (Child) ……(Parent) ……

Westbury-on-Severn CE Primary School
eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the ICT co-ordinator. This incident log will be monitored by the Headteacher.

Date & Time	Name of pupil or staff	Male Or Female	Computer or Class	Details of incident (including evidence)	Actions and Reasons

Flowchart for Managing an e-Safety Incident

Following an incident the ICT co-ordinator will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact the Headteacher immediately for advice:

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or videos containing child pornography
- Inciting racial or religious hatred
- Promoting illegal acts

Was illegal material or activity found or suspected?

Yes

Inform police and GLOS ICT Team and GSCB. Follow any advice given by the Police otherwise:
Confiscate any laptop or other device and if related to school network, disable user account.
Save ALL evidence but DO NOT view or copy. Let the Police review the evidence.
If a pupil is involved inform the Child Protection School Liaison Officer.
If a member of staff, contact the Local Authority Designated Officer for Allegations Management (LADO)

No

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to the member of staff or the ICT co-ordinator.

Flowchart for Managing an e-Safety Incident

If the incident did not involve any illegal activity then follow this flowchart

The ICT co-ordinator should:

- Record in the school e-Safety Incident Log
- Keep any evidence
- Inform Headteacher

Incident could be:

Using another person's username and password

Accessing websites which are against school policy eg games

Using a mobile phone to take videos during lessons

Using the technology to upset or bully

Did the incident involve a member of staff?

Yes

If member of staff has:

- behaved in a way that has or may have harmed a child;
- possibly committed a criminal offence;
- behaved towards a child in a way which indicates s/he is unsuitable to work with children;

contact the LADO If the incident does not satisfy the criteria in 10.1.1 of the GSCB procedures 2007 then follow points below.

Review evidence and determine if incident is accidental or deliberate

Decide on appropriate course of action

Follow school disciplinary procedures (if deliberate)

No

Was the child the victim or the instigator?

Victim

In-school action to support pupil by one or more of the following:
Class teacher
ICT co-ordinator
Headteacher
Designated CP officer
Inform parent/carer as appropriate
If the child is at risk inform CPSLO immediately

Instigator

Review incident and identify if other pupils were involved

Decide appropriate sanctions based on school rules/guidelines

Inform parents/carer if serious or persistent incident

In serious incidents consider informing the CPSLO as the child instigator could be at risk

Review school procedures/policies to develop practice.

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to the member of staff or the ICT co-ordinator.

Smile and Stay Safe Poster

E-Safety Rules to be displayed in class and on PC trolleys in school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.